



UNIVERSIDADE ESTADUAL PAULISTA
“JÚLIO DE MESQUITA FILHO”
Câmpus de São José do Rio Preto

Maria Fernanda Zordan Bonini

Teorema das Unidades de Dirichlet e o Reticulado
Logarítmico

São José do Rio Preto - SP
2023

Maria Fernanda Zordan Bonini

Teorema das Unidades de Dirichlet e o Reticulado
Logarítmico

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Financiadora: CAPES

São José do Rio Preto - SP
2023

B715t

Bonini, Maria Fernanda Zordan

Teorema das Unidades de Dirichlet e o Reticulado Logarítmico /
Maria Fernanda Zordan Bonini. -- São José do Rio Preto, 2023
197 p. : il., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp),
Instituto de Biociências Letras e Ciências Exatas, São José do Rio
Preto

Orientador: Antonio Aparecido de Andrade

1. Teoria algébrica dos números. 2. Teorema das unidades de
Dirichlet. 3. Unidades. 4. Anel de inteiros. 5. Reticulado Logarítmico.
I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de
Biociências Letras e Ciências Exatas, São José do Rio Preto. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Maria Fernanda Zordan Bonini

Teorema das Unidades de Dirichlet e o Reticulado
Logarítmico

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática, do Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista “Júlio de Mesquita Filho”, Câmpus de São José do Rio Preto.

Financiadora: CAPES

Comissão Examinadora

Prof. Dr. Antonio Aparecido de Andrade
Orientador

Prof. Dr. Edson Donizete de Carvalho
UNESP – Câmpus de Ilha Solteira

Prof. Dr. Leandro Bezerra de Lima
UFMS – Câmpus de Campo Grande

São José do Rio Preto - SP
28 de fevereiro de 2023

*A Deus e à minha família,
dedico.*

AGRADECIMENTOS

Tendo finalizado este trabalho, sinto que os agradecimentos que eu poderia fazer neste espaço não seriam suficientes para contemplar as pessoas que fizeram parte de todo o processo comigo. Espero que eu consiga, de alguma forma, expressar tamanha gratidão.

Agradeço primeiramente a Deus, que é minha maior força, por me ajudar a ultrapassar todos os obstáculos ao longo dessa caminhada. Juntamente, agradeço ao meu Anjo da Guarda, que nunca me deixou sozinha e, em nenhum momento, falhou em sua proteção.

Em seguida, quero agradecer a toda minha família e amigos.

Aos meus pais, Marcos e Sandra, meus maiores amores e exemplos. Vocês sempre foram e serão minha base; eu não teria chegado até onde cheguei sem o amor e apoio de vocês.

Às minhas irmãs, Ana Carolina e Vanessa, por toda amizade além da irmandade.

Às minha avós Aurora e Dalvina, e ao meu avô Elizeu, que mesmo sem entender direito o que eu faço, sempre se orgulharam de mim por ter seguido o caminho dos estudos.

Às minhas madrinhas Sônia e Simone, e ao meu padrinho Roberto, inspirações para mim, por continuamente me incentivarem na busca de conhecimento.

Aos meus primos Ana Paula e Thiago, meus grandes amigos desde a infância, por acreditarem no meu potencial sem precisar de prova.

À minha melhor amiga Maria Clara Lopes Taddone, que é minha companheira de todos os momentos e tornou esses anos muito mais felizes. Sua companhia foi essencial na minha vida.

Ao meu namorado Gabriel Radi, que foi um verdadeiro parceiro de caminhada, por me acalmar em todos os momentos de turbulência e não me deixar desanimar.

Às amigas Maria Clara, Mayara e Daiane, que foram minha família durante esses anos de mestrado. Agradeço por dividirem comigo tanto experiências da vida pessoal

quanto da vida acadêmica.

Às minhas amigas Ana Júlia e Yasmin, que além de confidentes e companheiras, me deram suporte sempre que precisei. Aos amigos Sérgio, Leone, Isaac, Neto e Murillo, que dividiram diversas tardes de estudos e tornaram esses momentos mais descontraídos.

Aos amigos que cultivei por todos esses anos, em especial aos que o Programa de Educação Tutorial (PET) me trouxe. Não consigo citar todos, mas saibam que vocês fizeram minha vida mais feliz.

Às minhas amigas Denise Bordin e Linara Facini, por terem sido sempre tão especiais e terem me ajudado tanto durante esses anos.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade, que é meu modelo de profissional e sempre esteve ao meu lado nessa trajetória de estudos; por ter tido fé em mim, incentivando, dando conselhos e ensinando.

Ao IBILCE, minha segunda casa, onde passei grande parte dos meus dias; foram anos de aprendizagem e conhecimento.

Aos professores que passaram pela minha caminhada de estudos, o tanto que aprendi com vocês é imensurável. Particularmente, aos professores Weber Pereira e Juliana Precioso, tutores do PET quando fiz parte do programa, por sempre estarem de portas abertas para nos acolher.

Aos professores e funcionários que passaram pela minha trajetória no Colégio Franciscano Coração de Maria, onde estudei desde os anos iniciais até o ensino médio. Em especial, à minha querida amiga Clara Poio, que me acompanhou por tantas fases da vida e continua presente ainda hoje.

Aos membros titulares e suplentes da Banca, Prof. Dr. Edson Donizete de Carvalho, Prof. Dr. Leandro Bezerra de Lima, Prof. Dr. Giliard Souza dos Anjos e Prof. Dr. Robson Ricardo de Araujo, por terem aceitado fazer parte desse momento tão importante para mim.

A todos que direta ou indiretamente colaboraram com este trabalho.

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

*O mistério da vida me causa a mais forte emoção.
É o sentimento que suscita a beleza e a verdade,
cria a arte e a ciência.*
ALBERT EINSTEIN [1]

RESUMO

Neste trabalho apresentamos resultados básicos da teoria algébrica dos números, entre eles traço, norma, discriminante e anel de inteiros algébricos. Estes serviram como base para encontrar as unidades (elementos invertíveis) de corpos de números, como o quadrático, cúbico e ciclotômico. Um artefato utilizado para encontrar as unidades dos corpos cúbicos foi o Teorema das Unidades de Dirichlet. Esse teorema representa o resultado mais significativo deste trabalho, fornecendo uma descrição quase completa em termos abstratos do grupo das unidades de um corpo de números, de modo a implicar que este grupo é finitamente gerado. Por fim, como aplicação deste teorema, apresentamos a construção dos reticulados logarítmicos, feitos a partir de um mergulho logarítmico restrito ao grupo das unidades do anel de inteiros algébricos de um corpo de números. Ainda, apresentamos uma cota superior para raio de cobertura deste reticulado através das unidades de um corpo ciclotômico.

Palavras-chave: Teoria algébrica dos números. Teorema das unidades de Dirichlet. Unidades. Anel de inteiros. Reticulado Logarítmico.

ABSTRACT

In this work, we present basic results of the algebraic number theory, among them trace, norm, discriminant, and ring of algebraic integers. These served as the basis for finding the units (invertible elements) of a number field, such as the quadratic, cubic, and cyclotomic. We used Dirichlet's Unit Theorem to find the cubic fields units. The mentioned theorem is the most significant result of this work, giving us an almost complete description of it in abstract terms of the group of units of a number field, implying that this group is finitely generated. Finally, as an application of this theorem, we have the construction of logarithmic lattices, made from a logarithmic homomorphism restricted to the group of units of the ring of algebraic integers of a number field. Also, we present an upper bound of the covering radius of this lattice through the units of a cyclotomic field.

Keywords: Algebraic number theory. Dirichlet's unit theorem. Units. Ring of integers. Logarithmic lattice.

Lista de Figuras

6.1	Reticulado $\mathbb{Z}^2$	165
6.2	Região fundamental do reticulado $\mathbb{Z}^2$	168
6.3	Representação das moedas colocadas por fileira	170
6.4	Cobertura esférica feita com o reticulado hexagonal	172
6.5	Região fundamental do reticulado hexagonal	173
6.6	Reticulado logarítmico associado a $\mathbb{Q}(\sqrt{3})$	178
6.7	$2x \leq \text{sen}(\pi x)$ no intervalo $[1/6, 1/2]$	180

Lista de Tabelas

2.1	Casos para análise do Anel de Inteiros de corpos cúbicos puros	46
3.1	Unidade fundamental e sua norma em $\mathbb{Q}(\sqrt{m})$	80
4.1	Valores da função de Euler $\varphi(k)$ para $k \leq 45$	120
4.2	Unidade fundamental em corpos cúbicos puros $\mathbb{Q}(\sqrt[3]{m})$	132
4.3	Unidade fundamental de corpos cúbicos com apenas uma imersão real . . .	133
4.4	Sistema de unidades fundamentais de corpos cúbicos totalmente reais . . .	134
4.5	Unidade fundamental de alguns corpos quárticos puros	136

Lista de Símbolos

$\mathbb{N}$	Conjunto dos Números Naturais
$\mathbb{Z}$	Conjunto dos Números Inteiros
$\mathbb{Q}$	Conjunto dos Números Racionais
$\mathbb{R}$	Conjunto dos Números Reais
$\mathbb{C}$	Conjunto dos Números Complexos
$a \equiv b \pmod{m}$	a e b são congruentes módulo m
$a \not\equiv b \pmod{m}$	a e b não são congruentes módulo m
$m \nmid n$	m não divide n
Σ	Somatório
Π	Produtório
$\mathbb{K}, \mathbb{L}, \mathbb{M}$	Corpos
$[\mathbb{L} : \mathbb{K}]$	Grau do corpo $\mathbb{L}$ sobre o corpo $\mathbb{K}$
$\text{Gal}(\mathbb{L} : \mathbb{K})$	Grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$
$\mathbb{Q}(\theta)$	Corpo de números com o elemento primitivo θ
$\mathcal{O}_{\mathbb{K}}$	Anel de inteiros do corpo $\mathbb{K}$
$U(\mathcal{O}_{\mathbb{K}})$ ou $\mathcal{O}_{\mathbb{K}}^*$	Grupo de Unidades do anel de inteiros $\mathcal{O}_{\mathbb{K}}$
$\bar{x}$	Conjugado complexo de x
$m_{\mathbb{K}}(\alpha)$	Polinômio minimal de α sobre $\mathbb{K}$
$p(x)$	Polinômio na variável x
$p'(x)$	Derivada do polinômio $p(x)$
$\deg(p(x))$	Grau do polinômio $p(x)$
$\text{Im}(\psi)$	Imagem da função ψ
$\ker(\psi)$	Núcleo da função ψ

$\langle a \rangle$ ou $a\mathcal{O}_{\mathbb{K}}$	Ideal gerado por a em $\mathcal{O}_{\mathbb{K}}$
$\mathbb{Z}_m$	Conjunto das classes residuais módulo m
$\det(\mathcal{M})$	Determinante da matriz $\mathcal{M}$
$N(\alpha)$ ou $N_{\mathbb{K}}(\alpha)$	Norma do elemento $\alpha \in \mathbb{K}$
$Tr(\alpha)$ ou $Tr_{\mathbb{K}}(\alpha)$	Traço do elemento $\alpha \in \mathbb{K}$
$D_{B/A}(\alpha_1, \dots, \alpha_n)$	Discriminante d $(\alpha_1, \dots, \alpha_n)$ de B sobre A
$D(f)$	Discriminante do polinômio f
$d(\mathbb{K})$	Discriminante do corpo $\mathbb{K}$
$\varphi(m)$	Função Phi de Euler aplicada a m
η	Unidade fundamental
$R(\mathbb{K})$	Regulador de $\mathbb{K}$
$\log$	Logaritmo na base 10
ζ_n	Raiz n -ésima da unidade
$\phi_n(x)$	n -ésimo polinômio ciclotômico
$\mathbb{Q}(\zeta_n)$	Corpo Ciclotômico gerado por ζ_n
$B_n(r)$	Bola n -dimensional centrada na origem e de raio r
Λ_B	Reticulado com base B
$\mathcal{P}_B$	Região fundamental do reticulado Λ sobre a base B
$Vol(\Lambda)$	Volume do reticulado Λ
$Vol(\mathcal{P})$	Volume da região fundamental $\mathcal{P}$
$(\Lambda_{\min})^2$	Norma mínima do reticulado Λ
ρ	Raio de empacotamento do reticulado Λ
$\Delta(\Lambda)$	Densidade de empacotamento associada ao reticulado Λ
$\delta(\Lambda)$	Densidade de centro associada ao reticulado Λ
$\mu(\Lambda)$	Raio de cobertura do reticulado Λ
$[a]$	Parte inteira de a
$\lceil a \rceil$	Inteiro maior ou igual a a
$A \oplus B$	Soma direta do grupo A com o grupo B
$o(G)$	Ordem do Grupo G
$T(G)$	subgrupo de torção do grupo G

Sumário

1	Introdução	15
2	Resultados básicos da teoria algébrica dos números	18
2.1	Anel de inteiros	18
2.2	Extensão algébrica	26
2.3	Norma e traço	33
2.4	Base integral	40
2.5	Discriminante	49
2.6	Unidades	61
3	Unidades em corpos quadráticos	63
3.1	Unidades de corpos quadráticos imaginários	63
3.2	Unidades de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2})$	65
3.3	A equação $x^2 - my^2 = 1$	67
3.4	Unidades de norma 1	72
3.5	Unidades de norma -1	76
3.6	Unidade fundamental	79
3.7	Calculando a unidade fundamental	89
4	Teorema das unidades de Dirichlet	99
4.1	Valorizações de elementos de um corpo de números	100
4.2	Teorema das unidades de Dirichlet	114
4.3	Sistema de unidades fundamentais	116
4.4	Raízes da unidade contidas em $\mathcal{O}_{\mathbb{K}}$	118
4.5	Unidades em corpos cúbicos	125
4.6	Regulador	136
5	Unidades em corpos ciclotômicos	141
5.1	Corpos ciclotômicos	141
5.2	Anel de inteiros de $\mathbb{Q}(\zeta_n)$	145
5.3	Unidades em corpos ciclotômicos	156
5.4	Unidades ciclotômicas	161
6	Reticulado logarítmico	164
6.1	Reticulados	164
6.2	Empacotamento esférico no $\mathbb{R}^n$	170
6.3	Mínimos sucessivos de um reticulado	174
6.4	Reticulado logarítmico	175

6.5	Raio de cobertura do reticulado logarítmico em $\mathbb{Q}(\zeta_n)$	179
7	Conclusão	187
	Referências	188
A	- Apêndice: Teorema Fundamental de Grupos Abelianos Finitamente Gerados	190
A.1	Decomposição de grupos abelianos livres finitamente gerados	190
	Índice Remissivo	196

1 Introdução

A Teoria Algébrica dos Números é uma área clássica e fascinante da Matemática. No início de seus estudos, não se havia um fim prático específico. Entretanto, atualmente a Teoria dos Números, assim como a Álgebra, tem diversas aplicações, dentre elas na Teoria da Informação, códigos e criptografias.

A Teoria da Informação surgiu com o matemático Claude E. Shannon, a partir da publicação do artigo *A Mathematical Theory of Communication* [2]. A partir deste momento, houve uma junção entre a Matemática (em especial, da Teoria dos Números) e a Engenharia Elétrica, com o objetivo de garantir uma transmissão de mensagens que fosse segura e eficiente, por meio dos canais de comunicação. Assim, surge a Teoria de Códigos Corretores de Erros, que permitem uma melhor qualidade na transmissão de sinais e dados. Além disso, as criptografias garantem a segurança e sigilo da mensagem e dos dados.

Uma das estruturas matemáticas de fundamental importância na teoria dos códigos corretores de erros são os reticulados, que são subgrupos discretos de pontos do $\mathbb{R}^n$. Os reticulados surgiram a partir de um problema geométrico como cobrir da melhor maneira possível o espaço euclidiano com esferas idênticas de forma que quaisquer duas esferas apenas se tangenciem e ocupem o maior espaço possível. Este problema é conhecido como empacotamento esférico no espaço euclidiano n -dimensional. Há uma importante relação entre empacotamento esférico e a Teoria de Códigos, que se explicita no fato de que o problema de encontrar empacotamentos esféricos densos em um dado espaço (isto é, esferas dispostas no espaço, de modo que ocupem a maior fração desse espaço) é equivalente a encontrar códigos corretores de erros eficientes, o que permite associar o estudo dos códigos aos reticulados e surgiram várias famílias de reticulados.

O presente texto tem como objetivo de fazer o estudo do grupo de unidades de corpos de números específicos, como meta gerar reticulados logarítmicos, que são definidos a partir do grupo de unidades do anel de inteiros de corpos de números.

Este estudo têm diversas aplicabilidades tanto em códigos quanto em criptografia. Pode se encontrar em [3] e [4] a dependência da capacidade de canais de desvanecimento em bloco com o raio de cobertura do reticulado logarítmico. Em [5] é mostrado que o reticulado logarítmico é eficientemente decodificável quando o corpo é ciclotômico de ordem igual a uma potência de primo, o que pode ser utilizado para atacar problemas em criptografia baseados no Problema do Ideal Principal. Ainda em [5] é dado um limitante superior para o raio de cobertura na norma infinito do reticulado logarítmico associado a corpos ciclotômicos de ordem igual a uma potência de primo, com alta probabilidade. Nesta dissertação apresentaremos uma generalização deste limite superior feita em [6], onde é dada uma cota superior para o reticulado logarítmico de qualquer corpo ciclotômico.

No Capítulo 2, apresentamos alguns pré-requisitos que são utilizados no decorrer deste trabalho. As principais referências neste capítulo são [7], [8] e [9]. Dividido entre 6 seções, o objetivo foi trazer resultados essenciais para compreender os capítulos posteriores. Iniciamos, na Seção 2.1, apresentando o importante conceito de elemento inteiro e anel de inteiros. Na Seção 2.2, introduzimos as extensões algébricas e os corpos de números, elementos que são utilizados reiteradamente durante todo desenvolvimento. Na Seção 2.3, apresentamos as definições e principais resultados de norma e traço e, em seguida, na Seção 2.4 introduzimos o conceito de base integral, colocando exemplos como a base integral de um corpo quadrático e de um corpo cúbico. Na Seção 2.5, apresentamos o conceito de discriminante e alguns resultados que facilitam seu cálculo. Por fim, na Seção 2.6, apresentamos algumas definições e propriedades das unidades, que é o nosso principal objeto de estudo.

No Capítulo 3, iniciamos o estudo das unidades em corpos quadráticos e as principais bibliografias são [8] e [10]. A Seção 3.1 é dedicada as unidades em corpos quadráticos imaginários, que são mais simples de ser determinados. Entretanto, quando consideramos corpos quadráticos reais, o trabalho não é tão simples. Começamos esta análise na Seção 3.2, fazendo um caso particular, e calculando o grupo das unidades de $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. O objetivo geral é determinar as unidades de $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, com m um inteiro positivo livre de quadrados. Este estudo está vinculado a equação de Pell, dada por $x^2 - my^2 = \pm 1$. Fizemos uma breve análise das soluções desta equação na Seção 3.3. Dando continuidade as unidades em corpos quadráticos, primeiro analisamos as unidades com norma 1 na Seção 3.4 e, em seguida, as unidades de norma -1 na Seção 3.5. Este estudo foi essencial para introduzir o conceito de unidade fundamental, apresentado na Seção 3.6. Por fim, apesar de termos apresentados alguns casos de como calcular a unidade fundamental η para alguns corpos de números, ainda não foi apresentado como encontrar a unidade fundamental η de um corpo quadrático $\mathbb{Q}(\sqrt{m})$, com m inteiro positivo livre de quadrados qualquer. Este problema foi endereçado a Seção 3.7, que apresentamos um algoritmo de como encontrar essas unidades através da expansão de $\sqrt{m}$ em frações contínuas; onde para fazer uma revisão dos conceitos de frações contínuas, utilizamos a bibliografia [11].

Dando seguimento, no Capítulo 4, apresentamos o principal resultado deste trabalho, o *Teorema das Unidades de Dirichlet* (4.2.1) que apresenta, em termos abstratos, a caracterização do grupo de unidades de um corpo de números qualquer. A bibliografia utilizada para o desenvolvimento deste capítulo foi [8]. Na Seção 4.1, apresentamos resultados sobre valorizações de elementos de corpos de números, onde estes resultados são essenciais para a prova do Teorema 4.2.1, feita na Seção 4.2. Na Seção 4.3, apresentamos a definição de sistema de unidades fundamentais. Dando continuidade, na Seção 4.4, apresentamos as raízes da unidade contidas no anel de inteiros do corpo de números $\mathbb{K}$, para isso fizemos uma breve revisão da função φ de Euler, e utilizamos a bibliografia [12]. Na Seção 4.5, apresentamos resultados sobre o grupo de unidades de corpos de números cúbicos, dando um limite inferior para a unidade fundamental em termos do discriminante do corpo $\mathbb{K}$. Finalmente, na Seção 4.6, apresentamos o conceito de regulador.

No Capítulo 5, apresentamos as unidades em corpos ciclotômicos. As principais bibliografias utilizadas foram [13], [14] e [15]. Na Seção 5.1, fizemos uma breve introdução sobre raízes da unidade e corpos ciclotômicos. Na Seção 5.2, apresentamos o anel de inteiros de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$ em três casos: $n = p$ primo, $n = p^r$ uma potência de primo e, por fim, para n um inteiro positivo qualquer. Na Seção 5.3, apresentamos resultados sobre unidades em corpos ciclotômicos. Por fim, na Seção 5.4, aprofundamos nas unidades ciclotômicas, que permitem uma categorização mais a fundo do grupo de

unidades de $\mathbb{Q}(\zeta_n)$.

Finalmente, no Capítulo 6, as principais referências utilizadas foram [7], [9], [6], [16], [17], [18] e [19]. Na Seção 6.1, fizemos a introdução do conceito de reticulados, apresentando suas principais definições e resultados. Em seguida, apresentamos o problema de empacotamento esférico no $\mathbb{R}^n$, dando exemplos de algumas coberturas esféricas. Definimos o conceito de mínimo sucessivo na Seção 6.3. Finalmente, na Seção 6.4, definimos o reticulado logarítmico, definido a partir de um homomorfismo utilizando a função log restrito ao grupo das unidades do anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números $\mathbb{K}$. Na Seção 6.5, finalizamos o capítulo apresentando o raio de cobertura do reticulado logarítmico em corpos ciclotômicos.

Ademais, no Apêndice A, apresentamos uma breve introdução sobre grupos abelianos finitamente gerados e provamos o *Teorema Fundamental dos Grupos Abelianos Finitamente Gerados*, que foi útil na demonstração do *Teorema das Unidades de Dirichlet*. Para isso, utilizamos as referências [13] e [20].

No Capítulo 7, apresentamos a conclusão deste trabalho e algumas perspectivas futuras de estudos. Outras referências foram utilizadas como apoio durante o desenvolvimento desta dissertação e foram citadas no final do trabalho, juntamente com as outras.

2 Resultados básicos da teoria algébrica dos números

Neste capítulo, apresentamos uma breve revisão sobre conceitos que são utilizados durante este trabalho, inserindo alguns dos resultados notórios de cada tópico. As principais referências utilizadas foram [7], [8] e [9]. Na Seção 2.1, apresentamos o conceito de elemento inteiro e anel de inteiros. Na Seção 2.2, introduzimos as extensões algébricas e os corpos de números, elementos que são utilizados reiteradamente durante todo desenvolvimento. Na Seção 2.3, apresentamos as definições e principais resultados de norma e traço e, em seguida, na Seção 2.4, introduzimos o conceito de base integral, colocando exemplos como a base integral de um corpo quadrático e de um corpo cúbico. Na Seção 2.5, apresentamos o conceito de discriminante e alguns resultados que facilitam seu cálculo. Finalmente, na Seção 2.6, apresentamos algumas definições e propriedades das unidades, que é o nosso principal objeto de estudo.

2.1 Anel de inteiros

Nesta seção, consideramos A e B dois anéis tal que A é subanel de B .

Definição 2.1.1. Um elemento $\alpha \in B$ é dito **inteiro** sobre A se α é raiz de um polinômio mônico com coeficientes em A , isto é, se existem $a_0, a_1, \dots, a_{n-1} \in A$, não todos nulos, tais que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0.$$

Observação 2.1.2. Sejam $B = \mathbb{C}$ e $A = \mathbb{Q}$. O elemento α da Definição 2.1.1 é chamado de **número algébrico**. Se $A = \mathbb{Z}$, então α é chamado **inteiro algébrico**.

Exemplo 2.1.3.

1. Todo elemento de A é inteiro sobre A . De fato: Para todo $\alpha \in A$, α é raiz de $x - \alpha \in A[x]$.
2. O elemento $\alpha = \frac{1}{2}(-1 + i\sqrt{3})$ é inteiro algébrico, pois é raiz do polinômio mônico $x^2 + x + 1$ com coeficientes em $\mathbb{Z}$.
3. $\alpha = \sqrt{2} \in \mathbb{C}$ é raiz do polinômio $x^2 - 2 \in \mathbb{Z}[x]$. Portanto, é um inteiro algébrico.
4. O elemento $\alpha = \frac{1}{\sqrt{2}} \in \mathbb{C}$ é um número algébrico, pois é raiz do polinômio mônico $x^2 - \frac{1}{2} \in \mathbb{Q}[x]$.

5. $\alpha = \frac{3\sqrt{2} - i\sqrt{2}}{2} \in \mathbb{C}$ é inteiro sobre $\mathbb{Z} + \mathbb{Z}i$, pois é raiz de $x^2 - (4 - 3i) \in (\mathbb{Z} + \mathbb{Z}i)[x]$.

6. $\alpha = \frac{1}{\sqrt{2}}$ não é um inteiro algébrico. De fato: Suponha que é um inteiro algébrico. Assim, existem coeficientes $a_0, a_1, \dots, a_{n-1} \in \mathbb{Z}[x]$ tais que

$$\left(\frac{1}{\sqrt{2}}\right)^n - (a_{n-1})\left(\frac{1}{\sqrt{2}}\right)^{n-1} + \dots + a_0 = 0.$$

Multiplicando por $(\sqrt{2})^n$, segue que

$$\frac{1}{(\sqrt{2})^n} \cdot (\sqrt{2})^n - (a_{n-1}) \cdot \frac{1}{(\sqrt{2})^n} (\sqrt{2})^n + \dots + a_0 (\sqrt{2})^n = 0.$$

Assim, $1 - a_{n-1}\sqrt{2} - a_{n-2}(\sqrt{2})^2 + \dots + a_0(\sqrt{2})^n = 0$, ou seja,

$$(1 + 2a_{n-2} + 4a_{n-4} + \dots) + \sqrt{2}(a_{n-1} + 2a_{n-3} + \dots) = 0.$$

Note que, se $a_{n-1} + 2a_{n-3} + \dots \neq 0$, então $\sqrt{2} = \frac{-(1 + 2a_{n-2} + 4a_{n-4} + \dots)}{(a_{n-1} + 2a_{n-3} + \dots)} \in \mathbb{Q}$, mas isso é um absurdo pois $\sqrt{2} \notin \mathbb{Q}$. Assim, $a_{n-1} + 2a_{n-3} + \dots = 0$, o que implica que $(\underbrace{1}_{\text{ímpar}} + \underbrace{2a_{n-2} + 4a_{n-4} + \dots}_{\text{par}}) = 0$, o que também é um absurdo. Portanto, $\frac{1}{\sqrt{2}} \in \mathbb{R}$ não é um inteiro algébrico.

Proposição 2.1.4. *Sejam $\beta \in B$ um inteiro sobre A e $\alpha \in A$. Assim, $\alpha\beta$ é inteiro sobre um subanel R de B que contém A .*

Demonstração. Se β é inteiro sobre A , então existem $a_0, \dots, a_{n-1} \in A$ tais que

$$\beta^n + a_{n-1}\beta^{n-1} + \dots + a_1\beta + a_0 = 0.$$

Seja $\alpha \in A \subseteq B$. Considere R um subanel de B . Logo, por ser subanel, $\alpha\beta \in R$. Assim,

$$\begin{aligned} \alpha^n(\beta^n + a_{n-1}\beta^{n-1} + \dots + a_1\beta + a_0) &= 0 \\ \Rightarrow (\alpha\beta)^n + a_{n-1}\alpha(\alpha\beta)^{n-1} + \dots + a_1\alpha^{n-1}(\alpha\beta) + a_0\alpha^n &= 0 \\ \Rightarrow (\alpha\beta)^n + a'_{n-1}(\alpha\beta)^{n-1} + \dots + a'_1(\alpha\beta) + a_0\alpha^n &= 0. \end{aligned}$$

Como $a_0, a'_i \in A$, para $i = 1, \dots, n-1$, segue que $\alpha\beta$ é inteiro sobre R . □

Proposição 2.1.5. *Considere a inclusão de anéis $A \subset B \subset C$. Se $\alpha \in C$ é inteiro sobre A , então α é inteiro sobre B .*

Demonstração. Se α é inteiro sobre A , então existem $a_0, \dots, a_{n-1} \in A$ tais que $p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$. Como $A \subset B$, segue que $a_0, \dots, a_{n-1} \in B$, ou seja, $p(x) \in B[x]$. Logo, α é inteiro sobre B . □

Definição 2.1.6. Seja $A \subset B$. Se para todo elemento α de B , α é inteiro sobre A , então dizemos que B é inteiro sobre A .

Corolário 2.1.7. *Sejam $A \subseteq B \subseteq C$ anéis. Se C é inteiro sobre A , então C é inteiro sobre B .*

Demonstração. Seja α um elemento inteiro sobre A . Pela Proposição 2.1.5, α é inteiro sobre B . Como vale para todo $\alpha \in C$, segue que C é inteiro sobre B . $\square$

Para o próximo teorema, precisamos das seguintes definições.

Definição 2.1.8. Um A -**módulo** M é um grupo aditivo com uma operação por escalar $\phi : A \times M \rightarrow M$, denotado por $(a, m) \mapsto \phi(a, u) = au$, tal que $\forall a, b \in A, u, v \in M$:

1. $(a + b)u = au + bu$;
2. $a(u + v) = au + av$;
3. $(ab)u = a(bu)$;
4. $1u = u$.

Definição 2.1.9.

1. Um A -módulo M é dito **finitamente gerado** se existe $\mathcal{B} = \{\alpha_i\}_{i \in I}$ finito tal que todo elemento de M pode ser escrito como uma combinação linear de $\mathcal{B}$. Notação: $M = \langle \mathcal{B} \rangle$.
2. Além disso, se $\mathcal{B}$ for linearmente independente, isto é, se $\sum_{i \in I} a_i \alpha_i = 0$ implicar que $a_i = 0$, para $i = 1, \dots, n$, o conjunto $\mathcal{B}$ forma uma base para M , que neste caso, M é chamado de **módulo livre**.

Observação 2.1.10. Seja $\alpha \in B$. O conjunto $A[\alpha] = \{f(\alpha) : f(x) \in A[x]\}$ é um A -módulo, e também, é o menor anel contido em B que contém α e A .

Teorema 2.1.11. *Seja α um elemento de B . As seguintes afirmações são equivalentes:*

1. α é inteiro sobre A .
2. O anel $A[\alpha]$ é um A -módulo finitamente gerado.
3. Existe um subanel R de B contendo A e α que é um A -módulo finitamente gerado.

Demonstração. Para $(1) \Rightarrow (2)$, como α é inteiro, segue que existem $a_0, a_1, \dots, a_{n-1} \in A$, não todos nulos, tais que

$$\alpha^n - a_{n-1}\alpha^{n-1} - \dots - a_1\alpha - a_0 = 0.$$

Seja M o submódulo de B gerado por $\{1, \alpha, \dots, \alpha^{n-1}\}$. Assim, $M \subseteq A[\alpha]$. Por outro lado,

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0) \in M.$$

Por indução, segue que $\alpha^{n+j} \in M$, para todo $j \geq 0$. Assim, $A[\alpha] \subseteq M$, e deste modo, $A[\alpha] = M$. Portanto, $A[\alpha]$ é um A -módulo finitamente gerado. Para $(2) \Rightarrow (3)$, basta tomar $R = A[\alpha]$. Finalmente, para $(3) \Rightarrow (1)$, considere um conjunto finito $\{\beta_1, \dots, \beta_n\}$ de geradores de R como um A -módulo. Assim,

$$R = A\beta_1 + \dots + A\beta_n.$$

Por hipótese, segue que $\alpha \in R$. Como R é um subanel de B , segue que $\alpha\beta_i \in R$, para todo $i = 1, \dots, n$. Desse modo, podemos escrever $\alpha\beta_i = \sum_{j=1}^n a_{i,j}\beta_j$, com $a_{i,j} \in A$ para $1 \leq i, j \leq n$. Logo,

$$\alpha\beta_i - \alpha\beta_i = \alpha\beta_i - \sum_{j=1}^n a_{i,j}\beta_j = 0 \Rightarrow \sum_{j=1}^n \left(\alpha \frac{\beta_i}{\beta_j} - a_{i,j} \right) \beta_j \stackrel{\frac{\beta_i}{\beta_j} = \delta_{i,j}}{\Rightarrow} \sum_{j=1}^n (\alpha\delta_{i,j} - a_{i,j})\beta_j = 0,$$

onde $i = 1, \dots, n$. Obtendo, assim, um sistema de n equações lineares homogêneas, dado por

$$\begin{cases} \sum_{j=1}^n (\alpha\delta_{1,j} - a_{1,j})\beta_j = 0 \\ \vdots \\ \sum_{j=1}^n (\alpha\delta_{n,j} - a_{n,j})\beta_j = 0. \end{cases}$$

Escrevendo na forma matricial, segue que

$$\begin{pmatrix} \alpha\delta_{1,1} - a_{1,1} & \alpha\delta_{1,2} - a_{1,2} & \cdots & \alpha\delta_{1,n} - a_{1,n} \\ \alpha\delta_{2,1} - a_{2,1} & \alpha\delta_{2,2} - a_{2,2} & \cdots & \alpha\delta_{2,n} - a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha\delta_{n,1} - a_{n,1} & \alpha\delta_{n,2} - a_{n,2} & \cdots & \alpha\delta_{n,n} - a_{n,n} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Seja d o determinante $\det(\delta_{i,j}\alpha - a_{i,j})$. Pela regra de Cramer,

$$\beta_i d = 0, \text{ onde } i = 1, \dots, n.$$

Portanto, $\beta \det(M) = 0$, para todo $\beta \in B$. Assim, $\det(M) = 0$. segue que $d\beta_i = 0$ para todo $i = 1, 2, \dots, n$. Como cada β_i gera B , segue que $B = \langle \beta_1, \dots, \beta_n \rangle$. Assim, segue que $dR = 0$. E em particular $d1 = d = 0$. Como o determinante é zero, segue que d é um polinômio mônico em α , onde o termo com ordem máxima aparece na expansão do produto

$$\prod_{i=1}^n (\delta_{i,i}\alpha - a_{i,i}) = \prod_{i=1}^n \left(\frac{\beta_i}{\beta_i} \alpha - a_{i,i} \right) = \prod_{i=1}^n (\alpha - a_{i,i})$$

das entradas da diagonal principal, ou seja, α é raiz de um polinômio mônico com coeficientes em A e, portanto, α é inteiro sobre A . $\square$

Proposição 2.1.12. *Seja $A \subseteq B \subseteq C$ uma inclusão de anéis. Se B é um A -módulo finitamente gerado e C é um B -módulo finitamente gerado, então C é um A -módulo finitamente gerado.*

Demonstração. Pela hipótese,

1. B é A -módulo f.g. e assim, existem $\beta_1, \dots, \beta_m$ tais que $B = A\beta_1 + \dots + A\beta_m$.
2. C é B -módulo f.g., e assim, existem $\alpha_1, \dots, \alpha_m$ tais que $C = B\alpha_1 + \dots + B\alpha_m$.

Considere $\alpha \in C$. Assim,

$$\alpha = \sum_{j=1}^n b_j \alpha_j, \text{ com } b_j \in B, \text{ onde } j = 1, \dots, n.$$

Por (1), segue que

$$\alpha = \sum_{j=1}^n \left(\sum_{i=1}^n a_{ij} \beta_i \right) \alpha_j, \text{ onde cada } a_{ij} \in A.$$

Logo, para todo $\alpha \in C$, segue que $\alpha = \sum_{j=1}^n \sum_{i=1}^n a_{ij} \beta_i \alpha_j$, ou seja, $C = A(\beta_1 \alpha_1) + A(\beta_2 \alpha_2) + \dots + A(\beta_n \alpha_n)$. Portanto, C é um A -módulo finitamente gerado. $\square$

Proposição 2.1.13. *Sejam $\alpha_1, \alpha_2, \dots, \alpha_n \in B$. Se α_1 é inteiro sobre A e α_i é inteiro sobre $A[\alpha_1, \dots, \alpha_{i-1}]$, para $i = 2, \dots, n$, então $A[\alpha_1, \alpha_2, \dots, \alpha_n]$ é um A -módulo finitamente gerado.*

Demonstração. Vamos provar por indução sobre n . Se $n = 1$, então α_1 é inteiro sobre A . Pelo Teorema 2.1.11, segue que $A[\alpha_1]$ é A -módulo finitamente gerado. Suponhamos que o resultado é válido para $n - 1$. Assim, α_i inteiro sobre A e α_i inteiro sobre $R = A[\alpha_1, \dots, \alpha_{n-1}]$ implicando que R é um A -módulo finitamente gerado. Mostremos que o resultado é válido para n . De R ser finitamente gerado, segue que existe um conjunto finito de geradores $\{\beta_1, \beta_2, \dots, \beta_p\}$ sobre A . Assim, $R = \sum_{j=1}^p A\beta_j$. Pelo Teorema 2.1.11, segue que $A[\alpha_1, \alpha_2, \dots, \alpha_n] = R[\alpha_n]$ é um R -módulo finitamente gerado. Desse modo, existe um conjunto finito de geradores sobre R dado por $\{\gamma_1, \gamma_2, \dots, \gamma_q\}$. Assim, todo elemento de $R[\alpha_n]$ é dado por $R[\alpha_n] = \sum_{k=1}^q R\gamma_k$. Daí,

$$A[\alpha_1, \alpha_2, \dots, \alpha_n] = R[\alpha_n] = \sum_{k=1}^q R\gamma_k \stackrel{R \text{ é f.g.}}{=} \sum_{k=1}^q \left(\sum_{j=1}^p A\beta_j \right) \gamma_k = \sum_{j,k} A\beta_j \gamma_k,$$

Note que $(\beta_j \gamma_k)$, onde $1 \leq j \leq p$ e $1 \leq k \leq q$, é um conjunto finito de geradores de $A[\alpha_1, \alpha_2, \dots, \alpha_n]$ como um A -módulo. Portanto, $A[\alpha_1, \alpha_2, \dots, \alpha_n]$ é um A -módulo finitamente gerado. $\square$

Corolário 2.1.14. *Se $\alpha_1, \alpha_2, \dots, \alpha_n$ são elementos de B que são inteiros sobre A , então $A[\alpha_1, \alpha_2, \dots, \alpha_n]$ é um A -módulo finitamente gerado.*

Demonstração. Como $A \subset A[\alpha_1, \dots, \alpha_n]$ e cada α_i é inteiro sobre A , segue que α_i é inteiro sobre $A[\alpha_1, \alpha_2, \dots, \alpha_{i-1}]$, para $i = 1, 2, \dots, n$. Desse modo, pela Proposição 2.1.13, podemos concluir que $A[\alpha_1, \alpha_2, \dots, \alpha_n]$ é um A -módulo finitamente gerado. $\square$

Proposição 2.1.15. *Se α e β são elementos de B que são inteiros sobre A , então $\alpha + \beta$, $\alpha - \beta$ e $\alpha\beta$ são inteiros sobre A .*

Demonstração. Como $A \subset B$ e $\alpha, \beta \in B$, segue que $A[\alpha, \beta]$ é um subanel de B . Claramente, $\alpha, \beta \in A[\alpha, \beta]$. Assim, $(\alpha + \beta)$, $(\alpha - \beta)$ e $(\alpha\beta)$ também pertencem a $A[\alpha, \beta]$. Agora, por α e β serem inteiros sobre A , pelo Corolário 2.1.14, segue que $A[\alpha, \beta]$ é um A -módulo finitamente gerado. Assim, obtemos um subanel $A[\alpha, \beta]$ de B que contém A , $\alpha + \beta$, $\alpha - \beta$ e $\alpha\beta$, que é um A -módulo finitamente gerado. Logo, pelo Teorema 2.1.11, segue que cada um desses elementos é inteiro sobre A . $\square$

Proposição 2.1.16. *Sejam A, B anéis tal que $A \subseteq B$. Se cada $\beta_1, \dots, \beta_n \in B$ é inteiro sobre A , então $A[\beta_1, \dots, \beta_n]$ é inteiro sobre um subanel R de B que contém A .*

Demonstração. Faremos essa prova por indução sobre n . Se $n = 1$, então β_1 é inteiro sobre A . Assim, existem $a_1, \dots, a_n \in A$ tais que

$$\beta_1^n + a_{n-1}\beta_1^{n-1} + \dots + a_1\beta_1 + a_0 = 0.$$

Seja R um subanel de B . Das Proposições 2.1.4 e 2.1.15, podemos garantir que $A[\beta_1]$ é inteiro sobre R , uma vez que valerá para quaisquer $a_i \in A$, onde $i = 1, \dots, n-1$. Agora, suponha que o resultado é válido para $n-1$, isto é, cada $\beta_1, \dots, \beta_{n-1}$ é inteiro sobre A e $A = [\beta_1, \dots, \beta_{n-1}]$ é inteiro sobre R . Queremos mostrar que o resultado é válido para n . Seja β_n um elemento inteiro de B sobre A . Assim, existem $x_1, \dots, x_n \in A[\beta_1, \dots, \beta_{n-1}]$ tal que

$$x_m(\beta_n)^m + \dots + x_1(\beta_n)^1 + x_0 = 0. \quad (2.1)$$

Note que o polinômio 2.1 pertence a $A[\beta_1, \dots, \beta_n]$. Da hipótese de indução, segue que cada $x_i \in A[\beta_1, \dots, \beta_{n-1}]$ é inteiro sobre R , uma vez que todo conjunto é. Mas, pela Proposição 2.1.15, podemos concluir que $x_m(\beta_n)^m + \dots + x_1(\beta_n)^1 + x_0$ sempre será inteiro sobre R , independente dos coeficientes x_i . Portanto, todo x_i de $A[\beta_1, \dots, \beta_n]$ é inteiro sobre R . Logo, $A[\beta_1, \dots, \beta_n]$ é inteiro sobre R . $\square$

Proposição 2.1.17. *Considere a seguinte inclusão de anéis $A \subseteq B \subseteq C$. Se B é inteiro sobre A e $\alpha \in C$ é inteiro sobre B , então α é inteiro sobre A .*

Demonstração. Se $\alpha \in C$ é inteiro sobre B , então existem elementos $b_0, \dots, b_{n-1} \in B$ tal que $\alpha^n + b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0 = 0$. Logo, α é inteiro sobre $R = A[b_0, \dots, b_{n-1}]$. Como cada b_i pertence a B e B é inteiro sobre A , segue que b_i é inteiro sobre A , onde $i = 0, \dots, n-1$. Pelo Corolário 2.1.14, segue que R é um A -módulo finitamente gerado. Agora, como α é inteiro sobre R , pelo Teorema 2.1.11, segue que $R[\alpha]$ é inteiro sobre R . Mais ainda, α é inteiro sobre A , como queríamos demonstrar. $\square$

O próximo corolário mostra a relação transitiva de extensões inteiras.

Corolário 2.1.18. *Sejam $A \subseteq B \subseteq C$ anéis. Se C é inteiro sobre B e B é inteiro sobre A , então C é inteiro sobre A .*

Demonstração. A prova é direta pela Proposição 2.1.17, uma vez que vale para todo elemento $\alpha \in C$. $\square$

Definição 2.1.19. Sejam $A \subseteq B$ anéis. O conjunto dos elementos de B que são inteiros sobre A é dado por

$$\mathcal{O}_B = \{\alpha \in B \mid \alpha \text{ é inteiro sobre } A\},$$

e é chamado **fecho inteiro** de A ou **anel de inteiros** de A em B .

Exemplo 2.1.20. Se $A = B$, então $\mathcal{O}_A = A$.

Observação 2.1.21. Sejam $A \subseteq B$ anéis. O anel de inteiros $\mathcal{O}_B$ de A em B é um anel satisfazendo

$$A \subseteq \mathcal{O}_B \subseteq B.$$

De fato: Pela Proposição 2.1.15, segue que $\mathcal{O}_B$ é um subanel de B . Como todo elemento de A é inteiro sobre A , segue que $\mathcal{O}_B$ contém A .

Proposição 2.1.22. *Todo subanel de B que é um A -módulo finitamente gerado está contido em $\mathcal{O}_B$.*

Demonstração. Seja $R = \langle \alpha_1, \dots, \alpha_n \rangle$ um subanel de B que é um A -módulo finitamente gerado. Claramente se $\alpha \in R$, $A[\alpha]$ é finitamente gerado como A -módulo, uma vez que $\alpha = a_1\alpha_1 + \dots + a_n\alpha_n$, com $a_i \in A$. Assim, pelo Teorema 2.1.11, segue que α é inteiro sobre A e, portanto, $\alpha \in \mathcal{O}_B$. Como vale para todo $\alpha \in R$, R está contido em $\mathcal{O}_B$. $\square$

No próximo teorema, apresentamos uma relação entre o conceito de corpo e o anel de inteiros.

Teorema 2.1.23. *Seja B um domínio tais que B é inteiro sobre A . O anel B é um corpo se, e somente se, A é um corpo.*

Demonstração. Mostremos primeiramente que se o anel B é um corpo, então A também é um corpo. Para isso, precisamos mostrar que se $\alpha \in A$, então existe $\alpha^{-1} \in A$. Sejam B um corpo e $\alpha \in A$ tal que $\alpha \neq 0$. Como, por hipótese, B é inteiro sobre A , segue que $A \subseteq B$. Daí, se $\alpha \in A$, então $\alpha \in B$. Além disso, como $\alpha \neq 0$, segue que existe elemento inverso $\alpha^{-1} \in B$, uma vez que B é corpo. Logo, $\alpha \in B$ e possui inverso $\alpha^{-1} \in B$. Novamente da hipótese de B ser inteiro sobre A , segue que este elemento α^{-1} será raiz de um polinômio mônico em $A[x]$. Seja

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0 \in A[x] \text{ tal que } p(\alpha^{-1}) = 0.$$

Daí,

$$\begin{aligned} \alpha^{-n} + a_{n-1}\alpha^{-n+1} + \dots + a_1\alpha^{-1} + a_0 &= 0 \\ \stackrel{\cdot \alpha^n}{\Rightarrow} \alpha^{-n}\alpha^{n-1} + a_{n-1}(\alpha^{-n+1})\alpha^{n-1} + \dots + a_1\alpha^{n-1}\alpha^{-1}\alpha^{n-1} + a_0\alpha^{n-1} &= 0 \\ \Rightarrow (\alpha^{-1}) + a_{n-1} + \dots + a_1(\alpha^{n-2}) + a_0(\alpha^{n-1}) &= 0 \\ \Rightarrow \alpha^{-1} = -(a_{n-1} + \dots + a_1\alpha^{n-2} + a_0\alpha^{n-1}). \end{aligned}$$

Como $p(x) \in A[x]$, segue que cada $a_i \in A$, onde $i = 1, \dots, n-1$. Logo, $\alpha^{-1} \in A$. Assim, A é um corpo. Reciprocamente, suponha que A é um corpo e $\alpha \neq 0$ é elemento de B . Como α é um elemento de B e B é inteiro sobre A , pelo Teorema 2.1.11, segue que $A[\alpha]$ é um A -módulo finitamente gerado. Por A ser corpo, segue que $A[\alpha]$ é um espaço vetorial de dimensão finita sobre A . Agora, considere a seguinte aplicação:

$$\psi : \begin{cases} A[\alpha] & \rightarrow & A[\alpha] \\ y & \mapsto & \alpha y \end{cases} \quad (y \in A[\alpha]).$$

Provemos que ψ é uma transformação linear e uma bijeção. Para isso, considere $a, b \in A[\alpha]$. Primeiramente, note que ψ está bem definida, uma vez que

$$a = b \Rightarrow \alpha a = \alpha b \Rightarrow \psi(a) = \psi(b).$$

Para mostrar que é uma transformação linear, devemos mostrar que preserva a operação. Vejamos,

$$\psi(a + b) = \alpha(a + b) = \alpha a + \alpha b = \psi(a) + \psi(b)$$

$$\psi(\beta a) = \alpha(\beta a) = \beta(\alpha a) = \beta\psi(a).$$

Por fim, para mostrar que é bijetiva, note que

$$y \in \ker(\psi) \Leftrightarrow \alpha y = 0 \stackrel{\alpha \neq 0}{\Leftrightarrow} y = 0, \text{ isto é, } \ker(\psi) = \{0\}.$$

Portanto, ψ é injetora. Além disso, como $A[\alpha]$ é um espaço vetorial de dimensão finita, segue que toda transformação linear é bijetora. Dessa forma, todo elemento de $A[\alpha]$ pode ser escrito como αa e, assim, garantimos também que ψ é sobrejetiva. Logo, é bijetora. Agora, como $1 \in A[\alpha]$, segue que existe $\beta \in A[\alpha] \subseteq B$ tal que $\alpha\beta = 1$, ou seja, α é inversível em B . Logo, concluímos que B é um corpo. $\square$

Definição 2.1.24. O anel A é chamado **integralmente fechado** em B quando $\mathcal{O}_B = A$. Se A é um domínio e $\mathbb{K}$ é o seu corpo de frações, o anel A é chamado integralmente fechado se $\mathcal{O}_{\mathbb{K}} = A$.

Proposição 2.1.25. *Sejam A um domínio e $\mathbb{K}$ o seu corpo de frações. O anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de A é integralmente fechado.*

Demonstração. Seja $\mathcal{O}'_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathcal{O}_{\mathbb{K}}$, isto é,

$$\mathcal{O}'_{\mathbb{K}} = \{\alpha \in \mathbb{K} \mid \alpha \text{ é inteiro sobre } \mathcal{O}_{\mathbb{K}}\}.$$

Por definição, segue que $\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}'_{\mathbb{K}}$. Assim, se $\alpha \in \mathbb{K}$, com α inteiro sobre $\mathcal{O}_{\mathbb{K}}$, então $\alpha \in \mathcal{O}'_{\mathbb{K}}$. Como vale a seguinte cadeia de inclusões,

$$A \subseteq \mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}'_{\mathbb{K}} \subseteq \mathbb{K},$$

pela Proposição 2.1.17, segue que α é inteiro sobre A . Portanto, $\mathcal{O}'_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$, garantindo que $\mathcal{O}_{\mathbb{K}} = \mathcal{O}'_{\mathbb{K}}$, ou seja, $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado. $\square$

Teorema 2.1.26. *Se A é um domínio principal, então A é integralmente fechado.*

Demonstração. Seja $\mathbb{K}$ o corpo de frações de A . Seja $\alpha \in \mathbb{K}$. Se α é inteiro sobre A , então $\alpha = \frac{a}{b}$, $b \neq 0$, $a, b \in A$ e $\text{mdc}(a, b) = 1$. Além disso, existem $a_0, a_1, \dots, a_{n-1}$ tais que

$$\begin{aligned} a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n &= 0 \\ \xRightarrow{\alpha = \frac{a}{b}} a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n &= 0 \\ \Rightarrow a_0 + a_1\left(\frac{a}{b}\right) + \dots + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \left(\frac{a}{b}\right)^n &= 0 \\ \xRightarrow{\cdot(b^n)} a_0b^n + a_1ab^{n-1} + \dots + a_{n-1}b + a^n &= 0 \\ \Rightarrow a^n = b(-a_0b^{n-1} - a_1ab^{n-2} - \dots - a_{n-1}a^{n-1}). \end{aligned}$$

Assim, $b|a^n$. Como $\text{mdc}(a, b) = 1$, segue que $b|a$. Assim, existe $u \in A$ tal que

$$a = ub \Rightarrow \alpha = \frac{a}{b} = u \in A.$$

Dessa forma, $\mathcal{O}_{\mathbb{K}} \subseteq A$. Como A é um domínio, segue que A está contido no anel de inteiros do seu corpo de frações, isto é, $A \subseteq \mathcal{O}_{\mathbb{K}}$. Logo, $\mathcal{O}_{\mathbb{K}} = A$. Portanto, pela Definição 2.1.24, A é integralmente fechado. $\square$

Exemplo 2.1.27. O anel $\mathbb{Z}$ é integralmente fechado, uma vez que é um domínio principal.

2.2 Extensão algébrica

A seguir, apresentamos alguns conceitos de extensões de corpos algébricas que utilizamos no restante do trabalho.

Definição 2.2.1. Sejam R um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq R$. Um elemento $\alpha \in R$ é dito **algébrico** sobre $\mathbb{K}$ se for raiz de um polinômio com coeficientes em $\mathbb{K}$. Caso contrário, α é chamado **transcendente** sobre $\mathbb{K}$.

Definição 2.2.2. Se α é algébrico sobre $\mathbb{K}$, então o polinômio mônico $m_\alpha(x)$ de grau mínimo tal que $m_\alpha(\alpha) = 0$ é chamado **polinômio minimal** de α sobre $\mathbb{K}$.

Definição 2.2.3. Sejam R um anel e $\mathbb{K}$ um corpo. O conjunto dos elementos de R que são algébricos sobre $\mathbb{K}$ é chamado **fecho algébrico** de $\mathbb{K}$ em R e denotado por $\mathcal{O}_{\mathbb{K}}$.

Definição 2.2.4. Sejam R um anel e $\mathbb{K}$ um corpo tal que $\mathbb{K} \subseteq R$. O anel R é chamado **algébrico** sobre $\mathbb{K}$ se todo elemento de R é algébrico sobre $\mathbb{K}$. Se R é um corpo, R é chamado uma **extensão algébrica** de $\mathbb{K}$.

Observação 2.2.5. Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos.

1. O fecho algébrico de $\mathbb{K}$ em $\mathbb{L}$ é igual a $\mathbb{L}$ se, e somente se, $\mathbb{L}$ é uma extensão algébrica sobre $\mathbb{K}$.
2. Todo elemento algébrico sobre $\mathbb{K}$ é um elemento inteiro sobre $\mathbb{K}$. Em particular, sobre corpos, elementos algébricos e inteiros são equivalentes.

Exemplo 2.2.6. O elemento $\alpha = \sqrt{7} - \sqrt{3}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio $x^4 - 20x^2 + 16$ com coeficientes em $\mathbb{Q}$. Note que esse elemento também poderia ser chamado de número algébrico pelas Observações 2.1.2 e 2.2.5.

Definição 2.2.7. Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos tal que $\mathbb{K} \subseteq \mathbb{L}$. Chamamos de **grau** de $\mathbb{L}$ sobre $\mathbb{K}$, a dimensão da extensão de $\mathbb{L}$ sobre $\mathbb{K}$ e denotamos por $[\mathbb{L} : \mathbb{K}]$.

Apresentamos, a seguir, algumas outras definições que são relevantes. Para isso, sejam $\mathbb{K}$ e $\mathbb{L}$ corpos tal que $\mathbb{K} \subseteq \mathbb{L}$ e seja $\alpha \in \mathbb{L}$.

1. O menor anel contido em $\mathbb{L}$ que contém α e $\mathbb{K}$ é definido por $\mathbb{K}[\alpha]$.
2. O menor corpo contido em $\mathbb{L}$ que contém α e $\mathbb{K}$ é definido por $\mathbb{K}(\alpha)$.

Além disso,

1. $\mathbb{K}[\alpha] \subseteq \mathbb{K}(\alpha)$.
2. $\mathbb{K}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{K}[x]\}$.
3. $\mathbb{K}(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in \mathbb{K}[x] \text{ e } g(\alpha) \neq 0 \right\}$.

Observe que se a extensão que estamos considerando é dada por $\mathbb{L} = \mathbb{K}(\alpha)$ de $\mathbb{K}$, com α um número algébrico sobre $\mathbb{K}$, podemos concluir que

$$\beta \in \mathbb{K}(\alpha) \Leftrightarrow \beta = a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}, \text{ com } a_i \in \mathbb{K}, \text{ onde } i = 1, \dots, n \text{ e } n = [\mathbb{K}(\alpha) : \mathbb{K}].$$

Assim, obtemos o seguinte resultado.

Proposição 2.2.8. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$ de grau n . Se $\alpha \in \mathbb{C}$ é algébrico sobre $\mathbb{K}$, então*

$$\mathbb{K}(\alpha) = \{a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mid \text{com } a_i \in \mathbb{K}, \text{ onde } i = 1, \dots, n\}.$$

A seguir, vamos provar uma proposição que é de extrema importância.

Proposição 2.2.9. *Toda extensão finita é algébrica.*

Demonstração. Considere a extensão de corpos $\mathbb{K} \subseteq \mathbb{L}$. Como é finita por hipótese, segue que $[\mathbb{L} : \mathbb{K}] = m < \infty$. Tome $\alpha \in \mathbb{L}$. Como $\mathbb{K}[\alpha]$ é um subespaço de $\mathbb{L}$, segue que $[\mathbb{K}(\alpha) : \mathbb{K}] = n \leq m$. Assim, o conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^n\}$ é um conjunto linearmente dependente, e portanto, α é algébrico sobre $\mathbb{K}$. Portanto, $\mathbb{L}$ é uma extensão algébrica. $\square$

Teorema 2.2.10. *Sejam $\mathbb{K}$, $\mathbb{L}$ e $\mathbb{M}$ corpos. Se $\mathbb{M}$ é uma extensão algébrica finita de $\mathbb{L}$ e $\mathbb{L}$ é uma extensão algébrica finita de $\mathbb{K}$, então $\mathbb{M}$ é uma extensão algébrica finita de $\mathbb{K}$, e assim,*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Demonstração. Considere $\{\alpha_1, \alpha_2, \dots, \alpha_m\}$ uma base de $\mathbb{M}$ sobre $\mathbb{L}$ e $\{\beta_1, \beta_2, \dots, \beta_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Verifiquemos que $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$. Se $\alpha \in \mathbb{M}$, então $\alpha = a_1\beta_1 + a_2\beta_2 + \dots + a_n\beta_n$, onde $a_j \in \mathbb{L}$, para $j = 1, 2, \dots, n$. Como cada $a_j \in \mathbb{L}$, segue que podemos escrevê-lo como $a_j = b_{1j}\alpha_1 + b_{2j}\alpha_2 + \dots + b_{mj}\alpha_m$, onde $b_i \in \mathbb{K}$, para $i = 1, 2, \dots, m$. Assim,

$$\alpha = \sum_{j=1}^n a_j\beta_j = \sum_{i,j} b_{i,j}\alpha_i\beta_j, \text{ onde } b_{i,j} \in \mathbb{K}.$$

Logo, $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$ gera $\mathbb{M}$ sobre $\mathbb{K}$. Agora, note que

$$\sum_{i,j} b_{i,j}\alpha_i\beta_j = 0 \Rightarrow \sum_{j=1}^n \left(\sum_{i=1}^m b_{i,j}\alpha_i \right) \beta_j = 0.$$

Como $\beta_1, \beta_2, \dots, \beta_n$ formam uma base, segue que são linearmente independentes. Assim, $\sum_{i=1}^m b_{i,j}\alpha_i = 0$. Analogamente, como $\alpha_1, \alpha_2, \dots, \alpha_m$ formam uma base, segue que são linearmente independentes, segue que $b_{i,j} = 0$ para todo $i = 1, 2, \dots, m$ e $j = 1, 2, \dots, n$. Dessa forma, $\{\alpha_1\beta_1, \dots, \alpha_m\beta_n\}$ é linearmente independente. Portanto, é uma base de $\mathbb{M}$ sobre $\mathbb{K}$ e podemos concluir que

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}],$$

o que prova o teorema. $\square$

Definição 2.2.11. *Seja $\mathbb{L}$ uma extensão do corpo $\mathbb{Q}$. Se o grau de $\mathbb{L}$ sobre $\mathbb{Q}$ é finito, o corpo $\mathbb{L}$ é chamado um **corpo de números algébrico**, ou simplesmente **corpo de números** ou **corpo numérico**.*

Definição 2.2.12. *Sejam $\mathbb{L}$ e $\mathbb{M}$ extensões de um corpo $\mathbb{K}$.*

1. Dois elementos $\alpha, \beta \in \mathbb{L}$ são chamados **conjugados** se são raízes do mesmo polinômio minimal.

2. Dois elementos $\alpha \in \mathbb{L}$ e $\beta \in \mathbb{M}$ são chamados **conjugados** sobre $\mathbb{K}$ se existe um $\mathbb{K}$ -isomorfismo ϕ de $\mathbb{K}(\alpha)$ em $\mathbb{K}(\beta)$ tal que $\phi(\alpha) = \beta$.

Definição 2.2.13. Sejam $\mathbb{L}$ e $\mathbb{M}$ extensões de um corpo $\mathbb{K}$. Os corpos $\mathbb{L}$ e $\mathbb{M}$ são **conjugados** sobre $\mathbb{K}$, ou são $\mathbb{K}$ -isomorfos, se existe um $\mathbb{K}$ -isomorfismo σ de $\mathbb{L}$ em $\mathbb{M}$ tal que $\sigma(a) = a$, para todo $a \in \mathbb{K}$.

Definição 2.2.14. Seja $\mathbb{K}$ um corpo. O corpo $\mathbb{K}$ tem **característica** m se $m\alpha = 0$, para todo elemento $\alpha \in \mathbb{K}$, e m é o menor inteiro positivo com esta propriedade. Se $m\alpha \neq 0$ para todo elemento não nulo α e inteiro positivo m , o corpo $\mathbb{K}$ tem característica zero.

Observação 2.2.15. Um corpo possui um único subcorpo minimal, chamado subcorpo primo, e este é isomorfo a $\mathbb{Q}$ ou a $\mathbb{Z}_p$, onde p é primo. Se é isomorfo a $\mathbb{Q}$ o corpo tem característica zero, e se é isomorfo a $\mathbb{Z}_p$, o corpo tem característica p .

Teorema 2.2.16. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$. Se $\alpha \in \mathbb{C}$ é algébrico sobre $\mathbb{K}$, então os conjugados de α sobre $\mathbb{K}$ são distintos.*

Demonstração. Suponha que α tenha dois conjugados sobre $\mathbb{K}$ iguais. Considere $m_{\mathbb{K}}(\alpha)$ o polinômio minimal de α sobre $\mathbb{K}$. Assim, $m_{\mathbb{K}}(\alpha)$ tem uma raiz de multiplicidade 2. Seja $\beta \in \mathbb{C}$ essa raiz. Assim,

$$m_{\mathbb{K}}(\alpha) = (x - \beta)^2 \cdot r(x),$$

onde $r(x) \in \mathbb{C}[x]$. Dessa forma,

$$m'_{\mathbb{K}}(\alpha) = 2(x - \beta)r(x) + (x - \beta)^2 r'(x).$$

Logo, β é uma raiz de $m'_{\mathbb{K}}(\alpha)$ e de $m_{\mathbb{K}}(\alpha)$. Além disso, como $m'_{\mathbb{K}}(\alpha) \in \mathbb{K}[x]$, segue que

$$m'_{\mathbb{K}}(\alpha) \in I_{\mathbb{K}}(\alpha) = \langle m_{\mathbb{K}}(\alpha) \rangle \Rightarrow m_{\mathbb{K}}(\alpha) \mid m'_{\mathbb{K}}(\alpha) \Rightarrow \deg(m_{\mathbb{K}}(\alpha)) \leq \deg(m'_{\mathbb{K}}(\alpha)),$$

o que é um absurdo, uma vez que $m'_{\mathbb{K}}(\alpha)$ é a derivada de $m_{\mathbb{K}}(\alpha)$. Portanto, os conjugados de α sobre $\mathbb{K}$ são distintos. $\square$

Teorema 2.2.17. *Se α é um inteiro algébrico, então seus conjugados sobre $\mathbb{Q}$ também são inteiros algébricos.*

Demonstração. Se α é inteiro algébrico, então existem $a_i \in \mathbb{Z}$, onde $i = 1, \dots, n-1$ tais que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0.$$

Note que $h(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ e $h(\alpha) = 0$. Considere $m_{\mathbb{K}}(\alpha)$ o polinômio minimal de α sobre $\mathbb{K}$. Assim,

$$h(x) \in I_{\mathbb{Q}}(\alpha) = \langle m_{\mathbb{Q}}(\alpha) \rangle \Rightarrow h(x) = m_{\mathbb{Q}}(\alpha) \cdot q(x), \text{ com } q(x) \in \mathbb{Q}[x].$$

Se β é um conjugado de α , então $m_{\mathbb{Q}(\alpha)}(\beta) = 0$, isto é, $h(\beta) = 0$ e, portanto, β é um inteiro algébrico. $\square$

Teorema 2.2.18. *Seja $\mathbb{K}$ um subcorpo de $\mathbb{C}$. Se $\alpha, \beta \in \mathbb{C}$ são algébricos sobre $\mathbb{K}$, então existe $\gamma \in \mathbb{C}$ algébrico sobre $\mathbb{K}$ tal que $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$.*

Demonstração. Seja $p(x)$ o polinômio minimal de α sobre $\mathbb{K}$ e $q(x)$ o polinômio minimal de β sobre $\mathbb{K}$. Assim,

$$\begin{aligned} p(x) &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) \in \mathbb{K}[x], \\ q(x) &= (x - \beta_1)(x - \beta_2) \cdots (x - \beta_n) \in \mathbb{K}[x], \end{aligned}$$

com $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_m$ conjugados de α sobre $\mathbb{K}$ e $\beta_1 = \beta, \beta_2, \dots, \beta_n$ conjugados de β sobre $\mathbb{K}$. Pelo Teorema 2.2.16, segue que $\alpha_i \neq \alpha_j, i \neq j$ e $\beta_i \neq \beta_j, i \neq j$. Considere o conjunto

$$S = \left\{ \frac{\alpha_r - \alpha_s}{\beta_t - \beta_u} \mid r, s = 1, \dots, m, \text{ e } t, u = 1, \dots, n, t \neq u \right\}.$$

Note que S é um subconjunto finito de $\mathbb{C}$. Seja $c \in \mathbb{Q}, c \neq x$, para todo $x \in S$. A partir de c , podemos obter mn elementos distintos, dois a dois, da forma

$$\alpha_i + c\beta_j, \text{ onde } i = 1, \dots, m \text{ e } j = 1, \dots, n.$$

Seja $\gamma = \alpha_1 + c\beta_1 = \alpha + c\beta$. Defina $\mathbb{K}_1 = \mathbb{K}(\gamma)$. Defina também $p_1(x) = p(\gamma - cx) \in \mathbb{K}_1[x] = (\mathbb{K}(\gamma))[x]$. Como $p_1(\beta) = p(\underbrace{\gamma - c\beta}_{\alpha}) = p(\alpha) = 0$ e $q(\beta) = 0$, segue que β é raiz de $p_1(x)$ e $q(x)$. Seja $\lambda \in \mathbb{C}$ uma raiz comum entre $p_1(x)$ e $q(x)$, com $\lambda \neq \beta$. Assim, $\lambda = \beta_j$, para algum $j = 2, \dots, n$. Assim,

$$p(\gamma - c\beta_j) = p_1(\beta_j) = 0.$$

Dessa forma, para algum $k = 1, \dots, m$, segue que $\alpha_k = \gamma - c\beta_j$. Logo,

$$\alpha_k + c\beta_j = \gamma = \alpha_1 + c\beta_1 \Rightarrow c(\beta_i - \beta_j) = \alpha_k - \alpha_1,$$

e assim,

$$c = \frac{\alpha_k - \alpha_1}{\beta_1 - \beta_j} \in S.$$

O que é absurdo, pois tomamos $c \notin S$. Portanto, a única raiz comum entre $p_1(x)$ e $q(x)$ é β . Agora, seja $h(x) = m_{\mathbb{K}_1}(\beta)$. Logo, $h(x)|p_1(x)$ e $h(x)|q(x)$. Como $p_1(x)$ e $h(x)$ possuem apenas uma raiz em comum em $\mathbb{C}$, segue que $\deg(h(x)) = 1$. De fato: Se $\deg(h(x)) \leq 2$ então existe uma outra raiz y tal que

$$\begin{aligned} h|p_1 &\Rightarrow p_1(x) = h(x)r(x) \Rightarrow p_1(y) = 0, \\ h|q &\Rightarrow q(x) = h(x)s(x) \Rightarrow q(y) = 0, \end{aligned}$$

o que são absurdos. Portanto, $h(x) = x + \delta$, para algum $\delta \in \mathbb{K}_1$. Assim,

$$\begin{aligned} h(\beta) &= 0 \Rightarrow \beta + \delta = 0 \Rightarrow \beta = -\delta \in \mathbb{K}_1 \\ \Rightarrow \alpha &= \underbrace{\gamma}_{\in \mathbb{K}_1} - c \underbrace{\beta}_{\in \mathbb{K}_1} \Rightarrow \mathbb{K}(\alpha, \beta) \subseteq \mathbb{K}(\gamma). \end{aligned}$$

Por outro lado, como $\gamma = \alpha + c\beta \in \mathbb{K}(\alpha, \beta)$, segue que $\mathbb{K}(\gamma) \subseteq \mathbb{K}(\alpha, \beta)$. Logo, $\mathbb{K}(\alpha, \beta) = \mathbb{K}(\gamma)$ e γ é algébrico sobre $\mathbb{K}$. $\square$

Corolário 2.2.19. *Seja $\mathbb{K}$ um subcorpo algébrico de $\mathbb{C}$. Se $\alpha_1, \dots, \alpha_n$ são algébricos sobre $\mathbb{K}$, então existe $\alpha \in \mathbb{C}$ algébrico tal que $\mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha)$.*

Demonstração. A prova segue por indução sobre n , aplicando o Teorema 2.2.18. $\square$

Teorema 2.2.20. (Teorema do Elemento Primitivo) Se $\mathbb{K}$ é um corpo de números algébrico, então existe um número algébrico θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$.

Demonstração. Por hipótese, segue que $\mathbb{K} = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$, com $\alpha_1, \dots, \alpha_n$ números algébricos. Pelo Corolário 2.2.19, existe $\theta \in \mathbb{C}$ algébrico sobre $\mathbb{Q}$ tal que $\mathbb{Q}(\alpha_1, \dots, \alpha_n) = \mathbb{Q}(\theta)$, isto é, $\mathbb{K} = \mathbb{Q}(\theta)$. $\square$

Observação 2.2.21. O elemento θ do Teorema 2.2.20 é chamado **elemento primitivo**.

Teorema 2.2.22. Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números algébrico, onde θ é um número algébrico. Se $\deg(m_{\mathbb{Q}}(\theta)) = n$, então todo elemento de $\mathbb{K}$ é expresso unicamente da forma $c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}$, com $c_i \in \mathbb{Q}$, onde $i = 1, \dots, n-1$ e cada um desses elementos pertence a $\mathbb{K}$.

Demonstração. Por hipótese, segue que $\mathbb{K} = \mathbb{Q}(\theta)$, com θ número algébrico e $\deg(m_{\mathbb{Q}}(\theta)) = n$. Pela Proposição 2.2.8, segue que

$$\mathbb{K} = \mathbb{Q}(\theta) = \{a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1} \mid a_0, \dots, a_n \in \mathbb{Q}\}.$$

Logo,

$$\alpha \in \mathbb{K} \Leftrightarrow \alpha = c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}, \text{ com } c_i \in \mathbb{Q}, \text{ onde } i = 1, \dots, n,$$

o que prova o resultado. $\square$

Observação 2.2.23. Um corpo de números algébrico $\mathbb{K} = \mathbb{Q}(\theta)$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão finita $n = \deg(m_{\mathbb{Q}}(\theta))$. Se $n = 2$, dizemos que $\mathbb{K}$ é corpo quadrático. Se $n = 3$, então $\mathbb{K}$ é um corpo cúbico. Se $n = 4$, então $\mathbb{K}$ é um corpo quártico.

A seguir, provamos um resultado essencial para este trabalho. Para isso, seja $\mathbb{K}$ um corpo de números algébricos. Nesta seção, começamos determinando o número de monomorfismos $\sigma : \mathbb{K} \rightarrow \mathbb{C}$. Um exemplo simples disso é o seguinte.

Exemplo 2.2.24. Se $\mathbb{K} = \mathbb{Q}(i)$, então i é um elemento algébrico, uma vez que é raiz do polinômio minimal $p(x) = x^2 + 1$. Desse modo, $\{1, i\}$ é uma base de $\mathbb{Q}(i)$ sobre $\mathbb{Q}$. Se $\alpha \in \mathbb{Q}(i)$, então $\alpha = a + bi$, com $a, b \in \mathbb{Q}$. Como $-i$ e i são raízes de $p(x)$, segue que os $\mathbb{Q}$ -monomorfismos são dados por

$$\sigma_1(a + bi) = a + bi$$

$$\sigma_2(a + bi) = a - bi.$$

Teorema 2.2.25. Se $\mathbb{K}$ é um corpo de números algébrico de grau n sobre $\mathbb{Q}$, então existem exatamente n monomorfismos $\sigma_k : \mathbb{K} \rightarrow \mathbb{C}$, onde $k = 1, \dots, n$.

Demonstração. Como $\mathbb{K}$ é um corpo de números algébrico, segue que existe um número algébrico $\theta \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. Assim, mostraremos que existem exatamente n $\mathbb{Q}$ -monomorfismos σ_k , onde $k = 1, \dots, n$. Considere $p(x) = m_{\mathbb{Q}}(\theta)$. Logo,

$$\deg(p(x)) = \deg(m_{\mathbb{Q}}(\theta)) = [\mathbb{Q}(\theta) : \mathbb{Q}] = n.$$

Assim, pelo Teorema 2.2.16, segue que θ tem n conjugados distintos sobre $\mathbb{Q}$. Se $\theta_1 = \theta, \theta_2, \dots, \theta_n$ são os conjugados de θ , então

$$p(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_n).$$

Ainda, pelo Teorema 2.2.22, segue que cada elemento $\alpha \in \mathbb{K}$ é expresso unicamente da forma $\alpha = a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}$, com $a_0, \dots, a_{n-1} \in \mathbb{Q}$. Para cada $k = 1, \dots, n$, defina

$$\sigma_k : \begin{cases} \mathbb{K} & \rightarrow \mathbb{C} \\ \alpha & \mapsto \sigma_k(\alpha) = a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1}. \end{cases}$$

1. Dados $\alpha, \beta \in \mathbb{K}$, segue que

$$\begin{aligned} \alpha &= a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}, \\ \beta &= b_0 + b_1\theta + \dots + b_{n-1}\theta^{n-1}, \end{aligned}$$

com $a_i, b_i \in \mathbb{Q}$, onde $i = 1, \dots, n-1$. Assim,

$$\begin{aligned} \alpha + \beta &= (a_0 + b_0) + (a_1 + b_1)\theta + \dots + (a_{n-1} + b_{n-1})\theta^{n-1} \Rightarrow \\ \sigma_k(\alpha + \beta) &= (a_0 + b_0) + (a_1 + b_1)\theta_k + \dots + (a_{n-1} + b_{n-1})\theta_k^{n-1} \\ &= a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} + b_0 + b_1\theta_k + \dots + b_{n-1}\theta_k^{n-1} \\ &= \sigma_k(\alpha) + \sigma_k(\beta). \end{aligned}$$

2. Para $\alpha, \beta \in \mathbb{K}$, considere

$$\begin{aligned} f(x) &= a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in \mathbb{Q}[x], \\ g(x) &= b_0 + b_1x + \dots + b_{n-1}x^{n-1} \in \mathbb{Q}[x], \end{aligned}$$

tais que $\alpha = f(\theta)$ e $\beta = g(\theta)$. Assim, existem $q(x), r(x) \in \mathbb{Q}[x]$ tal que

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

com $\deg(r(x)) < \deg(p(x)) = n$. Além disso, como $p(\theta) = 0$, segue que $\alpha\beta = f(\theta)g(\theta) = r(\theta)$. Agora, como $p(\theta_k) = 0$, segue que

$$\sigma_k(\alpha\beta) - \sigma(r(\theta)) = r(\theta_k) = p(\theta_k)q(\theta_k) + r(\theta_k) = f(\theta_k)g(\theta_k) = \sigma_k(\alpha)\sigma_k(\beta).$$

Portanto, de 1 e 2, segue que σ_k é homomorfismo, para $k = 1, \dots, n$.

3. Sejam $\alpha, \beta \in \mathbb{K}$ tais que

$$\begin{aligned} \alpha &= a_0 + \dots + a_{n-1}\theta^{n-1}, \quad a_i, b_i \in \mathbb{Q}. \\ \beta &= b_0 + \dots + b_{n-1}\theta^{n-1}, \quad \text{onde } i = 1, \dots, n-1. \end{aligned}$$

Logo,

$$\sigma_k(\alpha) = \sigma_k(\beta) \Rightarrow a_0 + \dots + a_{n-1}\theta_k^{n-1} = b_0 + \dots + b_{n-1}\theta_k^{n-1},$$

e assim,

$$(a_0 - b_0) + (a_1 - b_1)\theta_k + \dots + (a_{n-1} - b_{n-1})\theta_k^{n-1} = 0.$$

Desse modo, θ_k é uma raiz do polinômio

$$h(x) = (a_0 - b_0) + (a_1 - b_1)x + \dots + (a_{n-1} - b_{n-1})x^{n-1} \in \mathbb{Q}[x].$$

Assim, θ é raiz de $h(x)$. Note que $\deg(h(x)) = n-1 < n = \deg(p(x)) = \deg(m_{\mathbb{Q}}(\theta))$. Logo, $h(x)$ só pode ser o polinômio nulo. Logo, $a_i = b_i$, para todo $i = 1, \dots, n-1$. Portanto, $\alpha = \beta$. Desse modo, σ_k é injetiva, ou seja, σ_k é um monomorfismo, onde $k = 1, \dots, n$.

4. Considere $\lambda : \mathbb{K} \rightarrow \mathbb{C}$ um monomorfismo. Logo,

$$p(\lambda(\theta)) = \lambda(p(\theta)) = \lambda(0) = 0 \Rightarrow \lambda(\theta) = \theta_k, \text{ para algum, } k = 1, \dots, n.$$

Assim,

$$\begin{aligned} \lambda(\theta) = \sigma_k(\theta) &\Rightarrow \lambda(a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}) \\ &= a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} \\ &= \sigma_k(a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}), \forall a_0, a_1, \dots, a_{n-1} \in \mathbb{Q}. \end{aligned}$$

Portanto, $\lambda = \sigma_k$.

Assim, σ_k , para $k = 1, \dots, n$, são os únicos $\mathbb{Q}$ -monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. $\square$

Observação 2.2.26. Para $k = 1, \dots, n$, segue que

$$\begin{aligned} \text{Im}(\sigma_k) = \sigma_k(\mathbb{K}) &= \{\sigma_k(a_0 + \dots + a_{n-1}\theta^{n-1}) \mid a_i \in \mathbb{Q}\} \\ &= \{a_0 + a_1\theta_k + \dots + a_{n-1}\theta_k^{n-1} \mid a_i \in \mathbb{Q}\} \\ &= \mathbb{Q}(\theta_k), \end{aligned}$$

ou seja, $\sigma_k : \mathbb{Q}(\theta) \rightarrow \mathbb{Q}(\theta_k)$ é isomorfismo. Portanto, $\mathbb{Q}(\theta_i) \simeq \mathbb{Q}(\theta_j)$, onde $i, j = 1, \dots, n$.

Definição 2.2.27. Seja $\mathbb{K}$ um corpo de números algébrico. Sejam θ um número algébrico tal que $\mathbb{K} = \mathbb{Q}(\theta)$ e $\theta_1 = \theta, \theta_2, \dots, \theta_n$ são os conjugados de θ sobre $\mathbb{Q}$. Os corpos $\mathbb{Q}(\theta_1) = \mathbb{Q}(\theta) = \mathbb{K}, \dots, \mathbb{Q}(\theta_n)$ são chamados **corpos conjugados** de $\mathbb{K}$.

Pela Observação 2.2.26, segue que cada um dos corpos conjugados é isomorfo a $\mathbb{K}$. Mais ainda, eles não dependem do número algébrico θ tal que $\mathbb{K} = \mathbb{Q}(\theta)$. A seguir, vamos encontrar o anel de inteiros de alguns corpos em especial.

Teorema 2.2.28. Se $\mathbb{K}$ é um corpo quadrático, então existe um único $m \in \mathbb{Z}$, m livre de quadrados, tal que $\mathbb{K} = \mathbb{Q}(\sqrt{m})$.

Demonstração. Suponha que $\mathbb{K} = \mathbb{Q}(\sqrt{\alpha})$, onde α é raiz de um polinômio irredutível $p(x) = x^2 + ax + b \in \mathbb{Q}[x]$. Sejam α_1 e α_2 as raízes de $p(x)$. Neste caso, $\alpha = \alpha_1$ ou $\alpha = \alpha_2$, onde

$$\alpha_1 = \frac{-a + \sqrt{a^2 - 4ab}}{2} \text{ e } \alpha_2 = \frac{-a - \sqrt{a^2 - 4ab}}{2}.$$

Note que

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}\left(\frac{-a}{2} + \frac{1}{2}\sqrt{a^2 - 4b}\right) = \mathbb{Q}(\sqrt{a^2 - 4b}).$$

Analogamente,

$$\mathbb{Q}(\alpha_2) = \mathbb{Q}\left(\frac{-a}{2} - \frac{1}{2}\sqrt{a^2 - 4b}\right) = \mathbb{Q}(\sqrt{a^2 - 4b}),$$

ou seja, $\mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$. Portanto,

$$\mathbb{K} = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2) = \mathbb{Q}(\sqrt{c}), \text{ com } c = a^2 - 4b \in \mathbb{Q},$$

que, por sua vez, não tem raiz em $\mathbb{Q}$, uma vez que $x^2 + ax + b$ é irredutível sobre $\mathbb{Q}$. Considere $c = \frac{p}{q}$, com $p, q \in \mathbb{Z}$, $q > 0$ e $\text{mdc}(p, q) = 1$. Seja r^2 o maior quadrado que divide c . Assim, $c = r^2m$, com m inteiro livre de quadrados e $m \neq 1$. Além disso,

$$\mathbb{K} = \mathbb{Q}(\sqrt{c}) = \mathbb{Q}\left(\sqrt{\frac{p}{q}}\right) = \mathbb{Q}(\sqrt{r^2m}) = \mathbb{Q}(\sqrt{m}).$$

Agora, provamos que a unicidade. Para isso, seja $n \in \mathbb{Z}$ livre de quadrados, com $n \neq m$, tal que $\mathbb{Q}(\sqrt{n}) = \mathbb{K}$. Assim, $\mathbb{Q}(\sqrt{n}) = \mathbb{Q}(\sqrt{m})$. Assim, existem $x, y \in \mathbb{Q}$ tais que $\sqrt{m} = x + y\sqrt{n}$, isto é, $m = x^2 + 2xy\sqrt{n} + y^2n$.

- Se $xy \neq 0$, então $\sqrt{n} = \frac{m - x^2 - ny^2}{xy} \in \mathbb{Q}$, o que é um absurdo, pois $\sqrt{n} \notin \mathbb{Q}$. Assim, $xy = 0$ e $m = x^2 + y^2n$.
- Se $y = 0$, então $m = x^2 \Rightarrow \sqrt{m} \in \mathbb{Q}$, que é um absurdo. Assim, segue que $x = 0$. Logo, $m = y^2n$.

Como m é livre de quadrados, segue que $y = 1$ e, assim, $m = n$. Logo, existe um único $m \in \mathbb{Z}$, livre de quadrados, tal que $\mathbb{K} = \mathbb{Q}(\sqrt{m})$. $\square$

2.3 Norma e traço

A seguir, apresentamos a definição e principais resultados de norma e traço. Para isso, utilizamos noções de espaços vetoriais. Em particular, sobre módulos sobre anéis comutativos.

Seja A um anel e B um A -módulo livre finitamente gerado. Considere o seguinte endomorfismo $\varphi : B \rightarrow B$. Seja $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ uma base de B sobre A . Assim, definimos φ da seguinte forma:

$$\begin{cases} \varphi(e_1) = a_{11}e_1 + a_{12}e_2 + \dots + a_{1n}e_n \\ \varphi(e_2) = a_{21}e_1 + a_{22}e_2 + \dots + a_{2n}e_n \\ \vdots \\ \varphi(e_n) = a_{n1}e_1 + a_{n2}e_2 + \dots + a_{nn}e_n. \end{cases}$$

com $a_{ij} \in A$, para todo $i, j = 1, 2, \dots, n$. Podemos reescrever o endomorfismo φ na seguinte forma matricial.

$$\begin{bmatrix} \varphi(e_1) \\ \varphi(e_2) \\ \vdots \\ \varphi(e_n) \end{bmatrix} = \begin{bmatrix} a_{11}e_1 + a_{12}e_2 + \dots + a_{1n}e_n \\ a_{21}e_1 + a_{22}e_2 + \dots + a_{2n}e_n \\ \vdots \\ a_{n1}e_1 + a_{n2}e_2 + \dots + a_{nn}e_n \end{bmatrix} = [a_{ij}][e_j].$$

Definição 2.3.1.

1. O **traço** do endomorfismo φ é definido por

$$Tr_{B|A}(\varphi) = \sum_{i=1}^n a_{ii}.$$

2. A **norma** de φ é dada por

$$N_{B|A}(\varphi) = \det(a_{ij}).$$

3. O **polinômio característico** de φ é dado por

$$P_\varphi = \det(xI_n - \varphi) = \det(x\delta_{ij} - a_{ij}),$$

onde I_n é a matriz identidade de ordem n e $\delta_{ij} = 1$, se $i = j$ e $\delta_{ij} = 0$, se $i \neq j$.

Observação 2.3.2. Se φ e τ são dois endomorfismos, então

1. $Tr_{B|A}(\varphi + \tau) = Tr_{B|A}(\varphi) + Tr_{B|A}(\tau)$.
2. $N_{B|A}(\varphi\tau) = N_{B|A}(\varphi) \cdot N_{B|A}(\tau)$.
3. $\det(xI_n - \varphi) = x^n - [Tr_{B|A}(\varphi)] \cdot x^{n-1} + \dots + (-1)^n \cdot N_{B|A}(\varphi)$.

Agora, seja $A \subseteq B$ tal que B é um A -módulo livre finitamente gerado de posto n . Defina o endomorfismo $\varphi_\alpha : B \rightarrow B$ como dado por $\varphi_\alpha(x) = \alpha x$, com $\alpha \in B$.

Definição 2.3.3.

1. O **traço** de $\alpha \in B$ relativo a A é definido como o traço do endomorfismo φ_α e denotado por $Tr_{B|A}(\alpha) = Tr_{B|A}(\varphi_\alpha)$.
2. A **norma** de $\alpha \in B$ relativa a A é o determinante de φ_α e denotado por $N_{B|A}(\alpha) = \det(\varphi_\alpha)$.
3. O **polinômio característico** de $\alpha \in B$ relativo a A é definido como o polinômio característico do endomorfismo φ_α e denotado por $f_\alpha = \det(xI_n - \varphi_\alpha)$.

Definição 2.3.4. Sejam A e B anéis tal que $A \subseteq B$. O traço em B é dito **degenerado** se existe um elemento $\alpha \in B$, $\alpha \neq 0$, tal que $Tr_{B|A}(\alpha\beta) = 0$, para todo $\beta \in B$.

Observação 2.3.5. Se $\mathbb{K}$ é corpo de números e $\alpha \in \mathbb{K}$, então usamos a notação: $T_{\mathbb{K}}(\alpha)$ e $N_{\mathbb{K}}(\alpha)$. Ainda, se não houver risco de confusão entre os conjuntos A e B , usamos somente $Tr(\alpha)$ e $N(\alpha)$.

Observe que $Tr(\alpha)$ e $N(\alpha)$ são elementos de A e são calculados sobre elementos de B .

Observação 2.3.6. Sejam $A \subseteq B$ anéis tal que B é um A -módulo livre de posto finito (isto é, finitamente gerado). Se $\alpha, \beta \in B$ e $a \in A$, então

1. $\varphi_\alpha + \varphi_\beta = \varphi_{\alpha+\beta}$;
2. $\varphi_\alpha \cdot \varphi_\beta = \varphi_{\alpha\beta}$;
3. $\varphi_{a\alpha} = a\varphi_\alpha$.

Ainda, a matriz de φ_a em relação a uma base de B sobre A é uma matriz diagonal, onde a é a entrada de todas as diagonais.

Diretamente da Definição 2.3.1 e de resultados básicos de Álgebra Linear, podemos concluir as seguintes propriedades, onde $\mathbb{K} \subseteq \mathbb{L} \subseteq M$ são corpos e $[\mathbb{M} : \mathbb{K}] = n$. Se $\alpha, \beta \in \mathbb{M}$, então

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta)$.
2. $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha) = a Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$.
3. $Tr_{\mathbb{L}/\mathbb{K}}(a) = na$.
4. $N_{\mathbb{L}/\mathbb{K}}(a) = a^n$.
5. $N_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^n N_{\mathbb{L}/\mathbb{K}}(\alpha)$.

6. $N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\beta)$.
7. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = N_{\mathbb{M}/\mathbb{K}}(N_{\mathbb{L}/\mathbb{M}}(\alpha))$.
8. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = Tr_{\mathbb{M}/\mathbb{K}}(Tr_{\mathbb{L}/\mathbb{M}}(\alpha))$.

Note que, em geral

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta) \neq Tr_{\mathbb{L}/\mathbb{K}}(\alpha).Tr_{\mathbb{L}/\mathbb{K}}(\beta)$.
2. $N_{\mathbb{L}/\mathbb{K}}(\alpha + \beta) \neq N_{\mathbb{L}/\mathbb{K}}(\alpha) + N_{\mathbb{L}/\mathbb{K}}(\beta)$.

Exemplo 2.3.7. Considere o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{7})$.

1. $Tr(2.3) = Tr(6) = 12 \neq 24 = 4.6 = Tr(2).Tr(3)$.
2. $N(2 + 3) = N(5) = 25 \neq 13 = 4 + 9 = N(2) + N(3)$.

Teorema 2.3.8. Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão algébrica de grau $[\mathbb{L} : \mathbb{K}] = n$, com $\mathbb{K}$ finito ou de característica zero, e α um elemento de $\mathbb{L}$. Se $\alpha_1, \dots, \alpha_n$ são as raízes do polinômio minimal de α sobre $\mathbb{K}$, cada uma repetida $[\mathbb{L} : \mathbb{K}(\alpha)]$ -vezes, então

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^n \alpha_i = \alpha_1 + \dots + \alpha_n$,
2. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^n \alpha_i = \alpha_1 \dots \alpha_n$,
3. $m_\alpha(x) = \prod_{i=1}^n (x - \alpha_i) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$.

Além disso, o polinômio característico é a $[\mathbb{L} : \mathbb{K}(\alpha)]$ -ésima potência do polinômio minimal de α sobre $\mathbb{K}$.

Demonstração. Suponhamos que α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, $[\mathbb{L} : \mathbb{K}[\alpha]] = 1$ para $\mathbb{L} = \mathbb{K}[\alpha]$. Seja

$$m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0,$$

o polinômio minimal de α sobre $\mathbb{K}$ com $a_i \in \mathbb{K}$ para $i = 0, 1, \dots, n-1$. Como $\mathbb{L}$ é $\mathbb{K}$ -isomorfo a $\frac{\mathbb{K}[x]}{\langle m_\alpha(x) \rangle}$ e $\mathcal{B} = \{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que a matriz do endomorfismo

$$\varphi_\alpha : \begin{cases} \mathbb{L} & \rightarrow & \mathbb{L} \\ x & \rightarrow & x\alpha \end{cases}$$

com relação a $\mathcal{B}$ é dada por

$$\begin{cases} \varphi_\alpha(1) = \alpha \\ \varphi_\alpha(\alpha) = \alpha^2 \\ \vdots \\ \varphi_\alpha(\alpha^{n-1}) = \alpha^n \end{cases} \implies M = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix}.$$

Assim,

$$\begin{aligned} f_\alpha(x) &= \det(xI_n - \varphi_\alpha) = \det(xI_n - M) = \begin{vmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & \cdots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & x + a_{n-1} \end{vmatrix} \\ &= x^n + a_{n-1}x^{n-1} + \cdots + a_0 = m_\alpha(x). \end{aligned}$$

Mas, pela Observação 2.3.2, segue que

$$f_\alpha(x) = \det(xI_n - \varphi_\alpha(x)) = \det(xI_n - M) = x^n - (Tr_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha))x^{n-1} + \cdots + (-1)^n \det(\varphi_\alpha).$$

Agora, como α é primitivo, segue que o polinômio minimal é dado por

$$m_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) = x^n - \left(\sum_{i=1}^n \alpha_i \right) x^{n-1} + \cdots + (-1)^n \left(\prod_{i=1}^n \alpha_i \right).$$

Daí,

$$\begin{aligned} f_\alpha(x) &= m_\alpha(x) = x^n - (Tr_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha))x^{n-1} + \cdots + (-1)^n \det(\varphi_\alpha) \\ &= x^n - \left(\sum_{i=1}^n \alpha_i \right) x^{n-1} + \cdots + (-1)^n \left(\prod_{i=1}^n \alpha_i \right). \end{aligned}$$

Igualando os polinômios, segue que

$$\begin{cases} Tr_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^n \alpha_i, \\ N_{\mathbb{L}/\mathbb{K}}(\varphi_\alpha) = N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^n \alpha_i. \end{cases}$$

Desse modo,

$$Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^n \alpha_i, \quad N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^n \alpha_i \quad \text{e} \quad f_\alpha(x) = \prod_{i=1}^n (x - \alpha_i).$$

Por fim, faremos o caso geral, onde $[\mathbb{L} : \mathbb{K}[\alpha]] = m$. Note que é suficiente mostrarmos que o polinômio característico $f_\alpha(x)$ de α , com relação a $\mathbb{L}$ sobre $\mathbb{K}$, é igual a m -ésima potência do polinômio minimal de α sobre $\mathbb{K}$. Sejam $\{\alpha_1, \dots, \alpha_r\}$ uma base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ e $\{\beta_1, \dots, \beta_m\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}[\alpha]$. Assim, segue que $\{\alpha_1\beta_1, \dots, \alpha_r\beta_m\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ com $n = rs$, pois vale a multiplicidade dos graus. Considere $M = (a_{ih})$ a matriz do endomorfismo de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ com relação a base $(\alpha_i)_{1 \leq i \leq r}$. Logo,

$$\alpha\alpha_i = \sum_h (a_{ih})\alpha_h \xrightarrow{(\beta_j)} \alpha(\alpha_i\beta_j) = \left(\sum_h a_{ih}\alpha_h \right) \beta_j = \sum_h a_{ih}(\alpha_h\beta_j),$$

e assim,

$$\begin{cases} \alpha\alpha_1\beta_1 = a_{11}\alpha_1\beta_1 + a_{12}\alpha_2\beta_1 + \cdots + a_{1r}\alpha_r\beta_1 \\ \alpha\alpha_2\beta_1 = a_{21}\alpha_1\beta_1 + a_{22}\alpha_2\beta_1 + \cdots + a_{2r}\alpha_r\beta_1 \\ \vdots \\ \alpha\alpha_r\beta_1 = a_{r1}\alpha_1\beta_1 + a_{r2}\alpha_2\beta_1 + \cdots + a_{rr}\alpha_r\beta_1. \end{cases}$$

Agora, ordenamos a base $\{\alpha_1\beta_1, \dots, \alpha_r\beta_m\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, de modo que a matriz do endomorfismo seja da forma

$$M_1 = \begin{bmatrix} M & 0 & \cdots & 0 & 0 \\ 0 & M & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & M \end{bmatrix}.$$

Isto é, M se repete m -vezes na diagonal principal como blocos diagonais na matriz M_1 . Logo, a matriz $(xI_n - M_1)$, consiste em r blocos diagonais, cada um da forma $xI_r - M$. Assim,

$$xI_n - M_1 = \begin{bmatrix} xI_r - M & 0 & \cdots & 0 & 0 \\ 0 & xI_r - M & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & xI_r - M \end{bmatrix} \Rightarrow \det(xI_n - M_1) = \det(xI_r - M)^m.$$

Dessa forma, analogamente a primeira parte da demonstração, $f_\alpha(x) = \det(xI_n - M_1)$ é o polinômio característico de α sobre $\mathbb{K}$ e $\det(xI_r - M)$ é o polinômio minimal de α sobre $\mathbb{K}$, como queríamos demonstrar. $\square$

Observação 2.3.9. O Teorema 2.3.8 fornece a seguinte consequência direta, que pode ser útil em diversos momentos.

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = mTr_{\mathbb{K}[\alpha]/\mathbb{K}}(\alpha)$;
2. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = (N_{\mathbb{K}[\alpha]/\mathbb{K}}(\alpha))^m$;
3. $f_\alpha(x) = (m_\alpha(x))^m$.

Proposição 2.3.10. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações, onde $\mathbb{K}$ tem característica zero. Se $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e $\alpha \in \mathbb{L}$ é um elemento inteiro sobre A , então os coeficientes do polinômio característico f_α são inteiros sobre A . Em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são inteiros sobre A .*

Demonstração. Pela Proposição 2.3.8, segue que o polinômio característico de α é dado por $f_\alpha(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$, onde α_i é uma raiz do polinômio minimal de α . Pela relação de Girard, sabemos que os coeficientes de $f_\alpha(x)$ são, a menos de sinal, somas e produtos entre as raízes α_i de $f_\alpha(x)$. Assim, basta mostrar que todos α_i 's são inteiros sobre A , onde $i = 1, \dots, n$, e pela Proposição 2.1.15, segue o resultado. Como α_i é um conjugado de α sobre $\mathbb{K}$, segue que existe um $\mathbb{K}$ -isomorfismo $\sigma_i : \mathbb{K}[\alpha] \rightarrow \mathbb{K}[\alpha_i]$, definido por $\sigma_i(\alpha) = \alpha_i$. Como α é inteiro sobre A , segue que α é raiz de um polinômio em $A[x]$, isto é,

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0 \Rightarrow \sigma_i(\alpha)^n + a_{n-1}\sigma_i(\alpha)^{n-1} + \cdots + a_0 = 0,$$

e assim,

$$\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_1\alpha_i + a_0 = 0,$$

ou seja, α_i é inteiro sobre A , onde $i = 1, 2, \dots, n$. Portanto, os coeficientes de $f_\alpha(x)$ também serão inteiros sobre A . Pelo mesmo argumento, segue que $Tr_{\mathbb{L}/\mathbb{K}}$ e $N_{\mathbb{L}/\mathbb{K}}$ também são inteiros sobre A . $\square$

Corolário 2.3.11. *Se A é um anel integralmente fechado, então os coeficientes do polinômio característico $f_\alpha(x)$ são elementos de A . Em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de A .*

Demonstração. Todos os coeficientes de $f_\alpha(x)$ são elementos de $\mathbb{K}$. Pela Proposição 2.3.10, todos são inteiros sobre A . Como A é integralmente fechado, segue que os coeficientes a_i de $f_\alpha(x)$ pertencem a A , onde $i = 1, \dots, n$. Logo, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de A . $\square$

Proposição 2.3.12. *Seja $\mathbb{K}$ um corpo de números. Assim, $\alpha \in \mathbb{K}$ é um inteiro algébrico se, e somente se, seu polinômio característico tem coeficientes inteiros.*

Demonstração. Como α é um inteiro algébrico, pela Observação 2.1.2, segue que α é um inteiro sobre $\mathbb{Z}$, que por sua vez, é integralmente fechado. Assim, pelo Corolário 2.3.11, segue que os coeficientes do seu polinômio característico também são inteiros. Reciprocamente, por hipótese α tem o polinômio característico com coeficientes inteiros. Assim, $f_\alpha(\alpha) = 0$, ou seja, α é um inteiro algébrico. $\square$

Proposição 2.3.13. *Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$. Sejam $\{\alpha_1, \dots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$, onde $\det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)) \neq 0$ e $\alpha \in \mathbb{L}$. Se $Tr_{\mathbb{L}/\mathbb{K}}(\alpha \beta) = 0$, para todo $\beta \in \mathbb{L}$, então $\alpha = 0$.*

Demonstração. Se $\alpha \in \mathbb{L}$, então

$$\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n,$$

onde $a_i \in \mathbb{K}$, para $i = 1, \dots, n$. Assim, é suficiente mostrar que se $Tr_{\mathbb{L}/\mathbb{K}}(\alpha \alpha_j) = 0$, para cada $j = 1, \dots, n$, então $\alpha = 0$. Deste modo,

$$0 = Tr_{\mathbb{L}/\mathbb{K}}(\alpha \alpha_j) = a_1 Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_j) + a_2 Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2 \alpha_j) + \dots + a_n Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_j),$$

para cada $j = 1, \dots, n$. Colocando na forma matricial, segue que

$$\begin{bmatrix} Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_1) & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2 \alpha_1) & \dots & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_1) \\ Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_2) & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2 \alpha_2) & \dots & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_n) & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2 \alpha_n) & \dots & Tr_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)) \neq 0$, segue que $a_1 = a_2 = \dots = a_n = 0$. Portanto, $\alpha = 0$. $\square$

Corolário 2.3.14. *Considere $H_\alpha = Hom_{\mathbb{K}}(\mathbb{L} : \mathbb{K})$ dada por $H_\alpha(\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha \beta)$, com $\beta \in \mathbb{L}$. Assim, a aplicação $\psi : \mathbb{L} \rightarrow H_\alpha$ é um isomorfismo.*

Demonstração. Sejam $\alpha_1, \alpha_2 \in \mathbb{L}$. Assim, para todo $\beta \in \mathbb{L}$, segue que

- $\psi(\alpha_1 + \alpha_2) = H_{\alpha_1 + \alpha_2} = Tr_{\mathbb{L}/\mathbb{K}}((\alpha_1 + \alpha_2)\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha_1 \beta) + Tr_{\mathbb{L}/\mathbb{K}}(\alpha_2 \beta)$
 $= H_{\alpha_1}(\beta) + H_{\alpha_2}(\beta) = (\psi(\alpha_1) + \psi(\alpha_2))(\beta)$
- $\psi(a\alpha)(\beta) = H_{a\alpha}(\beta) = Tr_{\mathbb{L}/\mathbb{K}}(a\alpha\beta) = a Tr_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = a H_\alpha(\beta) = a\psi(\alpha)(\beta).$

Assim, ψ é um homomorfismo. Agora, se $\alpha \in \mathbb{L}$ é tal que $\rho(\alpha) = 0$, então

$$\psi(\alpha)(\beta) = H_\alpha(\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha \beta) = 0, \text{ para todo } \beta \in \mathbb{L}.$$

Pela Proposição 2.3.13, segue que $\alpha = 0$. Desse modo, ψ é injetora. Por fim, como $\dim_{\mathbb{K}} \mathbb{L} = \dim_{\mathbb{K}}(\text{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{K}))$, segue que ψ é sobrejetora. Portanto, ψ é um isomorfismo. $\square$

Teorema 2.3.15. *Se A é um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\mathcal{O}_{\mathbb{L}}$ o anel de inteiros de A em $\mathbb{L}$, então $\mathcal{O}_{\mathbb{L}}$ é um A -submódulo de um A -módulo livre.*

Demonstração. Considere $\{\alpha_1, \dots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Sabemos que toda extensão finita é algébrica pela Proposição 2.2.9. Assim, os α_i 's são algébricos sobre $\mathbb{K}$. Logo, existem a_i 's em A , onde $i = 1, \dots, n$, não todos nulos, tais que

$$a_n \alpha_i^n + a_{n-1} \alpha_i^{n-1} + \dots + a_0 = 0.$$

Sem perda de generalidade, suponha que $a_n \neq 0$. Assim,

$$\begin{aligned} a_n \alpha_i^n + a_{n-1} \alpha_i^{n-1} + \dots + a_0 &= 0 \xrightarrow{\cdot (a_n)^{n-1}} a_n^{n-1} (a_n \alpha_i^n + \dots + a_0) = 0 \\ \Rightarrow (a_n \alpha_i)^n + a_{n-1} (a_n \alpha_i)^{n-1} + \dots + a_n^{n-1} a_0 &= 0. \end{aligned}$$

Portanto, $a_n \alpha_i$ é inteiro sobre A , para $i = 1, \dots, n$. Agora, seja $a_n \alpha_i = \beta \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \dots, n$. Mostramos que $\{\beta_1, \dots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Suponha que

$$b_1 \beta_1 + b_2 \beta_2 + \dots + b_n \beta_n = 0, \quad \text{onde } b_i \in A, \quad \text{para } i = 1, \dots, n.$$

Logo,

$$b_1 a_n \alpha_1 + b_2 a_n \alpha_2 + \dots + b_n a_n \alpha_n = 0.$$

Como $\{\alpha_1, \dots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $b_i a_n = 0$, e portanto, $b_i = 0$ para $i = 1, \dots, n$. Portanto, $\{\beta_1, \dots, \beta_n\}$ é linearmente independente e, por possuir exatamente n elementos, segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 2.3.14, para $i, j = 1, \dots, n$, segue que existe uma base $\{\gamma_1, \dots, \gamma_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ tais que

$$\psi(\beta_i)(\gamma_j) = H_{\beta_i}(\gamma_j) = \text{Tr}_{\mathbb{L}/\mathbb{K}}(\beta_i \gamma_j) = \delta_{ij}.$$

Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $\alpha \beta_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, \dots, n$. Pelo Corolário 2.3.11, segue que $\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha \beta_i) \in A$, para $i = 1, \dots, n$. Assim,

$$\alpha = c_1 \gamma_1 + \dots + c_n \gamma_n, \quad \text{onde } c_i \in \mathbb{K}, \quad \text{para } i = 1, \dots, n,$$

e deste modo,

$$\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha \beta_i) = c_i \in A, \quad \text{onde } i = 1, \dots, n.$$

Portanto, $\mathcal{O}_{\mathbb{L}}$ é um submódulo de um A -módulo livre gerado por $\{\gamma_1, \dots, \gamma_n\}$. $\square$

Proposição 2.3.16.

1. *Se A é um anel principal, então $\mathcal{O}_{\mathbb{L}}$ é um A -módulo livre de posto n .*
2. *Além disso, se $I \subset \mathcal{O}_{\mathbb{L}}$ é um ideal, então I é um A -módulo livre de posto n .*

Demonstração. 1. Se A é um anel principal, então um submódulo livre é livre de posto menor ou igual a n . Pelo Teorema 2.3.15, segue que $\mathcal{O}_{\mathbb{L}}$ contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$ que possui n elementos, e assim, $\mathcal{O}_{\mathbb{L}}$ tem posto exatamente n .

2. Seja $I \subset \mathcal{O}_{\mathbb{L}}$ um ideal. Considere α um elemento não nulo de I e $\alpha_1, \alpha_2, \dots, \alpha_n$ uma base de $\mathcal{O}_{\mathbb{L}}$. Agora, observe que, para $1, \dots, n$

$$a_1 \alpha \alpha_1 + \dots + a_n \alpha \alpha_n + n = 0, a_i \in A \Rightarrow a_i \alpha = 0.$$

Como A é anel principal (e, assim é um domínio), segue que cada $a_i = 0$, para $i = 1, \dots, n$. Logo, $\{\alpha \alpha_1, \dots, \alpha \alpha_n\} \in I$ é linearmente independente sobre A . Assim, pela Definição 2.1.9, segue que I é um módulo livre de posto n , o que finaliza a prova da proposição. $\square$

A partir dos resultados gerais sobre traço e norma sobre anéis. A seguir, vamos apresentar um resultado que reescreve a Definição 2.3.1 para corpos de números e será muito útil no contexto deste trabalho.

Proposição 2.3.17. *Sejam $\mathbb{K}$ um corpo de números com $[\mathbb{K} : \mathbb{Q}] = n$ e $\sigma_1, \sigma_2, \dots, \sigma_n$ os n $\mathbb{Q}$ -monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Se $\alpha \in \mathbb{K}$, então*

1. O **traço** de α sobre $\mathbb{K}$ é dado por

$$Tr(\alpha) = \sum_{i=1}^n \sigma_i(\alpha).$$

2. A **norma** de α sobre $\mathbb{K}$ é dado por

$$N(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

3. O **polinômio característico** α sobre $\mathbb{K}$ é dado por

$$f_{\alpha} = \det(xI_n - \sigma_i(\alpha)),$$

onde I_n representa a matriz identidade de ordem n .

Demonstração. A demonstração segue direto da junção dos Teoremas 2.2.25 e 2.3.8. $\square$

2.4 Base integral

Nesta seção, apresentamos definições e propriedades de bases integrais de um corpo $\mathbb{K}$.

Proposição 2.4.1. *Sejam A um domínio, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão de $\mathbb{K}$. Se $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$, então existe $d \in A$, $d \neq 0$, tal que $d\alpha$ é inteiro sobre A .*

Demonstração. Se α é algébrico, então existem $a_0, a_1, \dots, a_{n-1} \in \mathbb{K}$ tais que $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$. Se d é o denominador comum dos a_i , então $da_i \in A$, para todo $i = 1, \dots, n-1$. Assim,

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n = 0 \xrightarrow{(d^n)} \\ a_0d^n + a_1d^n\alpha + \dots + a_{n-1}d^n\alpha^{n-1} + d^n\alpha^n = 0,$$

e assim,

$$a_0d^n + a_1d^{n-1}(d\alpha) + \dots + a_{n-1}d(d\alpha)^{n-1} + (d\alpha)^n = 0.$$

Como $a_0d^n, a_1d^{n-1}, \dots, a_{n-1}d \in A$, segue que $d\alpha$ é inteiro sobre A . $\square$

Proposição 2.4.2. *Um corpo de números $\mathbb{K}$ possui uma base formada por inteiros algébricos.*

Demonstração. Seja $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Pela Proposição 2.4.1, para cada $i = 1, 2, \dots, n$, existe $m_i \in \mathbb{Z}$, com $m_i \neq 0$, tal que $m_i \alpha_i$ é um inteiro algébrico. Desse modo, considere $m = m_1 m_2 \cdots m_n$. Claramente $m \neq 0$ e mais, $\{m \alpha_1, m \alpha_2, \dots, m \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ consistindo de inteiros algébricos. $\square$

Seja $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Seja o $\mathbb{Z}$ -módulo livre gerado por $\{m_1 \alpha_1, m_2 \alpha_2, \dots, m_n \alpha_n\}$, ou seja,

$$A = \mathbb{Z}m_1 \alpha_1 \oplus \cdots \oplus \mathbb{Z}m_n \alpha_n \subseteq \mathcal{O}_{\mathbb{K}}.$$

Pela Proposição 2.3.16, como $\mathbb{Z}$ é um anel principal, segue que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre de posto n . Dessa forma, existem $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathcal{O}_{\mathbb{K}}$ tais que todo elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ é escrito de modo único como

$$\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_n \alpha_n,$$

onde $a_1, a_2, \dots, a_n \in \mathbb{Z}$.

Com isso, concluímos o resultado a seguir.

Proposição 2.4.3. *Se $A = \mathbb{Z}$ e $\mathbb{K}$ é um corpo de números de grau n , então $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre de posto n .*

Definição 2.4.4. O conjunto $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subset \mathcal{O}_{\mathbb{K}}$ é chamado uma **base integral** de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ se todo elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ é escrito de modo único como

$$\alpha = a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_n \alpha_n,$$

onde $a_1, a_2, \dots, a_n \in \mathbb{Z}$.

Observação 2.4.5. Se $\mathbb{K}$ é um corpo de números tal que $[\mathbb{K} : \mathbb{Q}] = n$, então toda base integral $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, uma vez que o conjunto $\{\alpha_1, \alpha_2, \dots, \alpha_n\} \subset \mathcal{O}_{\mathbb{K}} \subseteq \mathbb{K}$ é linearmente independente sobre $\mathbb{Q}$ e possui n elementos.

Proposição 2.4.6. *Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros do corpo de números $\mathbb{K}$ de grau n . Todo ideal não nulo I de $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo finitamente gerado de posto n .*

Demonstração. Vejamos que I é um $\mathbb{Z}$ -submódulo de $\mathcal{O}_{\mathbb{K}}$. Como $\mathbb{Z}$ é principal, segue que I é um $\mathbb{Z}$ -módulo livre finitamente gerado de posto menor ou igual a n . Assim, pela Proposição 2.4.3, segue que I é um A -módulo livre de posto n . $\square$

Definição 2.4.7. Seja $\mathbb{K} = \mathbb{Q}(\alpha)$ um corpo de números de grau n , com $\alpha \in \mathbb{K}$. Se o conjunto $\mathcal{B} = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ forma uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, então $\mathcal{B}$ é chamado de **base potente** (ou base de potências).

No nosso contexto, é importante saber a base integral do corpo de números $\mathbb{K}$, pois ela nos permite encontrar o determinante, que veremos a seguir na Seção 2.5. Faremos alguns casos que serão mais importantes neste trabalho.

Primeiramente, vamos encontrar o anel de inteiros do corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, com m livre de quadrados.

Teorema 2.4.8. *Sejam $\mathbb{K}$ um corpo quadrático e $m \in \mathbb{Z}$ o único livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{m})$. O anel de inteiros, $\mathcal{O}_{\mathbb{K}}$, de $\mathbb{K}$ em $\mathbb{Z}$ é dado por*

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{se } m \not\equiv 1 \pmod{4}. \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right), & \text{se } m \equiv 1 \pmod{4}. \end{cases}$$

Demonstração. Considere

$$A = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{se } m \not\equiv 1 \pmod{4}. \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right), & \text{se } m \equiv 1 \pmod{4}. \end{cases}.$$

Queremos mostrar que $A = \mathcal{O}_{\mathbb{K}}$.

1. Seja $\alpha \in A$. Claramente $\alpha \in \mathbb{K}$.

(a) Se $m \not\equiv 1 \pmod{4}$, então $\alpha \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, isto é, $\alpha = a + b\sqrt{m}$, com $a, b \in \mathbb{Z}$. Assim,

$$\begin{aligned} \alpha^2 &= a^2 + b^2m + 2ab\sqrt{m} + 2a^2 - 2a^2 \\ &= a^2 + b^2m + 2a(a + b\sqrt{m}) - 2a^2 \\ &= -a^2 + b^2m + 2a\alpha. \end{aligned}$$

Isso implica que

$$\alpha^2 = 2a\alpha + (a^2 - b^2m) = 0, \text{ com } -2a \in \mathbb{Z}, \text{ e } a^2 - b^2m \in \mathbb{Z}. \quad (2.2)$$

Portanto, α é raiz do polinômio $x^2 - 2ax + (a^2 - b^2m) \in \mathbb{Z}[x]$. Logo, $\alpha \in \mathcal{O}_{\mathbb{K}}$.

(b) Se $m \equiv 1 \pmod{4}$, então $\alpha \in \left(\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)\right)$. Assim, $\alpha = a + b\left(\frac{1+\sqrt{m}}{2}\right)$, com $a, b \in \mathbb{Z}$. Daí,

$$\begin{aligned} \alpha^2 &= a^2 + 2ab\left(\frac{1+\sqrt{m}}{2}\right) + \left(\frac{b+b\sqrt{m}}{2}\right)^2 \\ &= a^2 + ab + ab\sqrt{m} + \frac{b^2}{4} + \frac{b^2\sqrt{m}}{2} + \frac{b^2m}{4} \\ &= 2a^2 - a^2 + ab + (ab - ab) + ab\sqrt{m} + \frac{b^2}{4} + \frac{b^2}{4} - \frac{b^2}{4} + \frac{b^2\sqrt{m}}{2} + \frac{b^2m}{4} \\ &= 2a^2 + ab + ab\sqrt{m} + ab + \frac{b^2}{2} + \frac{b^2\sqrt{m}}{2} - a^2 - ab + b^2\frac{(m-1)}{4} \\ &= 2a^2 + 2ab\left(\frac{1+\sqrt{m}}{2}\right) + ab + b^2\left(\frac{1+\sqrt{m}}{2}\right) - a^2 - ab + b^2\frac{(m-1)}{4} \\ &= \underbrace{(2a+b)a + b\left(\frac{1+\sqrt{m}}{2}\right)}_{\alpha} - a^2 - ab + b^2\frac{(m-1)}{4}. \end{aligned}$$

Isto implica que

$$\alpha^2 = (2a+b)\alpha - a^2 - ab + b^2\frac{(m-1)}{4} \Rightarrow \alpha^2 - (2a+b)\alpha + a^2 + ab - b^2\frac{(m-1)}{4} = 0.$$

Como $m \equiv 1 \pmod{4}$, segue que $4|m-1$ e, portanto, $b^2 \cdot \frac{(m-1)}{4} \in \mathbb{Z}$. Assim, α é raiz do polinômio

$$x^2 - (2a+b)x + \left(a^2 + ab - b^2 \frac{(m-1)}{4}\right) \in \mathbb{Z}[x].$$

Logo, $\alpha \in \mathcal{O}_{\mathbb{K}}$, e portanto, $A \subseteq \mathcal{O}_{\mathbb{K}}$.

2. Considere $\alpha \in \mathcal{O}_{\mathbb{K}}$. Queremos mostrar que $\alpha \in A$. Se $\alpha \in \mathcal{O}_{\mathbb{K}} \Rightarrow \alpha \in \mathbb{K} \Rightarrow \alpha = a + b\sqrt{m}$, com $a, b \in \mathbb{Q}$ e α raiz de um polinômio mônico em $\mathbb{Z}[x]$. Note que, se $\alpha = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$, então, de maneira análoga ao item 1, segue que α é raiz do polinômio $f(x) = x^2 - 2ax + (a^2 - mb^2) \in \mathbb{Q}[x]$. Assim,

$$\Delta = 4a^2 - 4(a^2 - mb^2) = 4b^2m.$$

Como m é livre de quadrados, segue que $f(x)$ é redutível em $\mathbb{Q}[x]$ se $b = 0$ e irreduzível em $\mathbb{Q}[x]$ se $b \neq 0$. Assim, o polinômio minimal de α em $\mathbb{Q}[x]$ é

$$m_{\mathbb{Q}}(\alpha) = \begin{cases} x - a, & \text{se } b = 0, \\ x^2 - 2ax + (a^2 - mb^2), & \text{se } b \neq 0; \end{cases}$$

Por hipótese, segue que α é um inteiro algébrico. Logo, pelo Teorema 2.3.12, segue que $m_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Logo,

$$\begin{cases} a \in \mathbb{Z}, & \text{se } b = 0, \\ 2a, a^2 - mb^2 \in \mathbb{Z}, & \text{se } b \neq 0. \end{cases}$$

- Se $b = 0$, então $\alpha = a \in \mathbb{Z} \subseteq \mathbb{Z} + \sqrt{m} \subseteq A$.
 - Se $b \neq 0$, então $2a \in \mathbb{Z}$ e $a^2 - mb^2 \in \mathbb{Z}$.
- (a) Suponha que $2a$ é par. Logo, $a \in \mathbb{Z}$ e $a^2 \in \mathbb{Z}$. Assim, como $a^2 - mb^2 \in \mathbb{Z}$, segue que $mb^2 \in \mathbb{Z}$. Seja $b = \frac{c}{d}$, com $c, d \in \mathbb{Z}$, $d \neq 0$ e $\text{mdc}(c, d) = 1$. Assim,

$$m \left(\frac{c}{d}\right)^2 \in \mathbb{Z} \Rightarrow d^2 | m.$$

Como m é livre de quadrados, segue que $d^2 = 1$ e, portanto, $d = \pm 1$, o que garante que $b \in \mathbb{Z}$. Logo, $a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m} \subseteq A$.

- (b) Agora, suponha que $2a$ é ímpar. Assim,

$$2a = 2k + 1, \quad k \in \mathbb{Z} \Rightarrow a = k + \frac{1}{2}, \quad k \in \mathbb{Z} \Rightarrow a^2 = k^2 + k + \frac{1}{4} \notin \mathbb{Z}.$$

Daí,

$$a^2 - mb^2 \in \mathbb{Z} \Rightarrow 4(a^2 - mb^2) \in \mathbb{Z},$$

e assim,

$$a^2 - mb^2 = 4 \left[\left(k + \frac{1}{2}\right)^2 - mb^2 \right] = 4 \left[k^2 + k + \frac{1}{4} - mb^2 \right] \in \mathbb{Z}.$$

Como $4k^2 + 4k + 1 \in \mathbb{Z}$, segue que $4mb^2 \in \mathbb{Z}$. Seja $2b = \frac{r}{s}$, com $r, s \in \mathbb{Z}$, $s \neq 0$ e $\text{mdc}(r, s) = 1$. Logo,

$$m(2b)^2 \in \mathbb{Z} \Rightarrow m \left(\frac{r}{s} \right)^2 \in \mathbb{Z} \Rightarrow s^2 | m.$$

Como m é livre de quadrados, segue que $s = \pm 1$, isto é, $2b \in \mathbb{Z}$. Agora, $2b$ pode ou não ser par. Se $2b$ é par, então $b \in \mathbb{Z}$ e, assim,

$$b^2 \in \mathbb{Z} \Rightarrow mb^2 \in \mathbb{Z} \Rightarrow \underbrace{(a^2 - mb^2)}_{\in \mathbb{Z}} + \underbrace{mb^2}_{\in \mathbb{Z}} \in \mathbb{Z} \Rightarrow a^2 \in \mathbb{Z}.$$

Mas, note que isso é um absurdo, pois estamos no caso em que $2a$ é ímpar. Portanto, $2b$ é ímpar e, assim, $2b = 2q + 1$. Assim,

$$a = \frac{2k + 1}{2} \text{ e } b = \frac{2q + 1}{2}, \text{ como } k, q \in \mathbb{Z}.$$

Logo,

$$\begin{aligned} a^2 - mb^2 &= \left(\frac{2k + 1}{2} \right)^2 - m \left(\frac{2q + 1}{2} \right)^2 = \frac{1}{4} [(2k + 1)^2 - m(2q + 1)^2] \\ &= \frac{1}{4} [4k^2 + 4k + 1 - m(4q^2 + 4q + 1)] \\ &= \frac{1}{4} [4k^2 + 4k + 1 - 4mq^2 - 4qm - m] \\ &= \frac{1}{4} [4(k^2 + k - mq^2 - mq) + 1 - m] \\ &= k^2 + k - mq^2 - mq + \frac{1 - m}{4} \in \mathbb{Z}. \end{aligned}$$

Desse modo,

$$\frac{m - 1}{4} = k^2 + k - mq^2 - mq - (a^2 - mb^2) \in \mathbb{Z}.$$

Portanto, $m \equiv 1 \pmod{4}$ e

$$\begin{aligned} \alpha &= a + b\sqrt{m} = \frac{2k + 1}{2} + \frac{2q + 1}{2}\sqrt{m} \\ &= \frac{2k + 1}{2} + \frac{2q + 1}{2}\sqrt{m} + \frac{2q + 1}{2} - \left(\frac{2q + 1}{2} \right) \\ &= (2q + 1) \left(\frac{1 + \sqrt{m}}{2} \right) + kq + \frac{1}{2} - \frac{1}{2} \\ &= \underbrace{(k - q)}_{\in \mathbb{Z}} + \underbrace{(2q + 1)}_{\in \mathbb{Z}} \left(\frac{1 + \sqrt{m}}{2} \right) \in \mathbb{Z} + \mathbb{Z} \left(\frac{1 + \sqrt{m}}{2} \right) \subseteq A. \end{aligned}$$

Logo, $\alpha \in A$.

Portanto, $\mathcal{O}_{\mathbb{K}} \subseteq A$. Assim, $\mathcal{O}_{\mathbb{K}} = A$. □

Corolário 2.4.9. *Seja $\mathbb{K}$ um corpo quadrático. Seja m um inteiro livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{m})$. Uma base integral de $\mathbb{K}$ é dada por*

1. *Se $m \not\equiv 1 \pmod{4}$, então $\{1, \sqrt{m}\}$.*
2. *Se $m \equiv 1 \pmod{4}$, então $\left\{1, \frac{1 + \sqrt{m}}{2}\right\}$.*

Demonstração. A demonstração segue direto da Definição de base integral (2.4.4) e do Teorema 2.4.8. $\square$

A seguir, apresentaremos o anel de inteiros de um corpo cúbico puro.

Teorema 2.4.10. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$, com $\theta = \sqrt[3]{m}$, m livre de quadrados. O anel de inteiros algébrico $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ é dado por*

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2, & \text{se } m \not\equiv \pm 1 \pmod{9}. \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - 2\theta + \theta^2}{3}\right), & \text{se } m \equiv 1 \pmod{9}. \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - \theta + \theta^2}{3}\right), & \text{se } m \equiv -1 \pmod{9}. \end{cases}$$

Demonstração. Suponha que $\alpha \in \mathbb{K}$ é um inteiro algébrico. Assim, $\alpha = a_0 + a_1\theta + a_2\theta^2$, com $a_1, a_2, a_3 \in \mathbb{Q}$. Pela Proposição 2.3.12, os coeficientes do polinômio característico devem ser inteiros. Calculando o polinômio característico do corpo cúbico puro e, sabendo que seus coeficientes devem ser inteiros, segue que $3a_0, 3a_1$ e $3a_2$ são inteiros. Suponha que $3a_i = p_i$, onde $i = 1, 2, 3$. Assim,

$$a_i = \frac{p_i}{3}, \quad \text{onde } i = 1, 2, 3.$$

Ainda, como cada p_i pode ser reescrito como $p_i = 3q_i + r_i$, com $q_i, r_i \in \mathbb{Z}$ e $r_i \in \{0, 1, 2\}$, para todo $i = 1, 2, 3$. Assim,

$$\begin{aligned} \alpha &= a_0 + a_1\theta + a_2\theta^2 = \frac{p_0}{3} + \frac{p_1}{3}\theta + \frac{p_2}{3}\theta^2 \\ &= \frac{3q_0 + r_0}{3} + \frac{3q_1 + r_1}{3}\theta + \frac{3q_2 + r_2}{3}\theta^2 \\ &= q_0 + q_1\theta + q_2\theta^2 + \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2. \end{aligned}$$

Considere $q = q_0 + q_1\theta + q_2\theta^2$ e $r = \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2$. Assim, $\alpha = q + r$. Como $\mathcal{O}_{\mathbb{K}}$ é um anel e $\alpha \in \mathcal{O}_{\mathbb{K}}$, segue que $q + r \in \mathcal{O}_{\mathbb{K}}$, isto é, $q \in \mathcal{O}_{\mathbb{K}}$ e $r \in \mathcal{O}_{\mathbb{K}}$. Dessa forma, α é inteiro algébrico se, e somente se, q e r são inteiros algébricos. Mas, note que q_0, q_1, q_2 são inteiros, e assim, o polinômio característico de q tem coeficientes inteiros. Assim,

$$\alpha \in \mathcal{O}_{\mathbb{K}} \text{ se, e somente se, } r \in \mathcal{O}_{\mathbb{K}}. \quad (2.3)$$

Observe que pela Proposição 2.3.12, segue que

$$r \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \begin{cases} 3 \left(\frac{r_0}{3} \right) \in \mathbb{Z}, \\ 3 \left(\frac{r_0}{3} \right)^2 - 3 \left(\frac{r_1}{3} \right) \left(\frac{r_2}{3} \right) m \in \mathbb{Z}, \\ \left(\frac{r_0}{3} \right)^3 - 3 \left(\frac{r_0}{3} \right) \left(\frac{r_1}{3} \right) \left(\frac{r_2}{3} \right) m + m \left[\left(\frac{r_1}{3} \right)^3 + \left(\frac{r_2}{3} \right)^3 m \right] \in \mathbb{Z}. \end{cases} \quad (2.4)$$

Desse modo, juntando as informações obtidas em (2.4) na expressão 2.3, segue que $\alpha \in \mathcal{O}_{\mathbb{K}}$ se, e somente se, os casos a seguir ocorrem

1. $\omega_1 = \frac{(r_0)^3 - r_1 r_2}{3} \in \mathbb{Z}.$
2. $\omega_2 = \frac{(r_0)^3 - 3r_0 r_1 r_2 m + m[(r_1)^3 + m(r_2)^3]}{27} \in \mathbb{Z}.$

Assim, listamos todas as possibilidades para m de acordo com os parâmetros r_0, r_1 e $r_2 \in \{0, 1, 2\}$. Observe que,

- Se $r_0 \neq 0$, $r_1 = 0$ ou $r_2 = 0$, então $\omega_1 \notin \mathbb{Z}$.
- Se $r = 0$, $r_1 = 0$ ou (exclusivo) $r_2 = 0$, então $\omega_1 = 0$ e ω_2 é um número inteiro que satisfaz $m \equiv 0 \pmod{9}$. Entretanto, m é livre de quadrados, o que implica que estes casos não possuem solução.

Na Tabela(2.4), apresentamos uma análise das linhas que possuem solução, ou seja, que existe $m \in \mathbb{Z}$ tal que $\omega_1, \omega_2 \in \mathbb{Z}$.

Linhas	r_0	r_1	r_2	ω_1	ω_2	$m \equiv (?) \pmod{9}$
1	0	0	0	0	0	Vale para todo m .
2	0	1	1	$\frac{-m}{3}$	$\frac{m+m^2}{27}$	Não existe m .
3	0	1	2	$\frac{-2m}{3}$	$\frac{m+8m^2}{27}$	Não existe m .
4	0	2	1	$\frac{-2m}{3}$	$\frac{8m+m^2}{27}$	Não existe m .
5	0	2	2	$\frac{-4m}{3}$	$\frac{8(m+m^2)}{27}$	Não existe m .
6	1	1	1	$\frac{1-m}{3}$	$\frac{(1-m)^2}{27}$	$m \equiv 1 \pmod{9}$
7	0	1	2	$\frac{1-2m}{3}$	$\frac{1-5m+8m^2}{27}$	Não existe m .
8	1	2	1	$\frac{1-2m}{3}$	$\frac{(1+m)^2}{27}$	$m \equiv -1 \pmod{9}$
9	1	2	2	$\frac{1-4m}{3}$	$\frac{1-4m+8m^2}{27}$	Não existe m .
10	2	1	1	$\frac{4-m}{3}$	$\frac{8-m+m^2}{27}$	Não existe m .
11	2	1	2	$\frac{4-2m}{3}$	$\frac{8-11m+8m^2}{27}$	$m \equiv -1 \pmod{9}$
12	2	2	1	$\frac{4-2m}{3}$	$\frac{8-4m+m^2}{27}$	Não existe m .
13	2	2	2	$\frac{4-4m}{3}$	$\frac{8(1-m)^2}{27}$	$m \equiv 1 \pmod{9}$

Tabela 2.1: Casos para análise do Anel de Inteiros de corpos cúbicos puros

Note que, a célula da tabela que consideramos "para todo m ", não inclui as equivalências não livre de quadrados, uma vez que m é livre de quadrados. Para as linhas que possuem

solução, analisamos os possíveis casos a seguir. Para essa análise, relembre da seguinte igualdade:

$$\alpha = q_0 + q_1\theta + q_2\theta^2 + \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2 \in \mathcal{O}_{\mathbb{K}}. \quad (2.5)$$

- $m \not\equiv 1 \pmod{9}$:

1. Na linha 1, os restos são $r_0 = 0, r_1 = 0$ e $r_2 = 0$. Assim, substituindo esses valores na Equação 2.5, segue que

$$\alpha = q_0 + q_1\theta + q_2\theta^2.$$

Como q_0, q_1 e $q_2 \in \mathbb{Z}$, segue que $\alpha \in \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$.

- $m \equiv 1 \pmod{9}$:

1. Na linha 6, os restos são $r_0 = 1, r_1 = 1$ e $r_2 = 1$. Assim,

$$\begin{aligned} \alpha &= q_0 + q_1\theta + q_2\theta^2 + \frac{1 + \theta + \theta^2}{3} \\ &= \left(q_0 + \frac{1}{3}\right) + \left(q_1 + \frac{1}{3}\right)\theta + \left(q_2 + \frac{1}{3}\right)\theta^2. \end{aligned} \quad (2.6)$$

Considere $A = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - 2\theta + \theta^2}{3}\right)$. Mostremos que $\mathcal{O}_{\mathbb{K}} = A$. Por definição, segue que $\alpha \in \mathcal{O}_{\mathbb{K}}$. Suponha que $\alpha \in A$. Assim, existem $z_0, z_1, z_2 \in \mathbb{Z}$ tais que

$$\begin{aligned} \alpha &= z_0 + z_1\theta + z_2\left(\frac{-2 - 2\theta + \theta^2}{3}\right) \\ &= \left(z_0 + \frac{2z_2}{3}\right) + \left(z_1 + \frac{2z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2. \end{aligned} \quad (2.7)$$

Pela igualdade de polinômios nas expressões (2.6) e (2.7), segue que

$$\begin{cases} z_0 - \frac{2z_2}{3} = q_0 + \frac{1}{3} \\ z_1 - \frac{2z_2}{3} = q_1 + \frac{1}{3} \\ \frac{z_2}{3} = q_2 + \frac{1}{3} \end{cases} \Rightarrow \begin{cases} z_0 = q_0 + 2q_2 + 1 \\ z_1 = q_1 + 2q_2 + 1 \\ z_2 = 3q_2 + 1. \end{cases}$$

Como $q_i \in \mathbb{Z}$, com $i = 1, 2, 3$, segue que $z_i \in \mathbb{Z}$, onde $i = 1, 2, 3$. Portanto, $\alpha \in A$. Assim, $\alpha \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \alpha \in A$, isto é, $\mathcal{O}_{\mathbb{K}} = A$.

2. Na linha 13, os restos são $r_0 = 2, r_1 = 2$ e $r_2 = 2$. Substituindo em (2.5),

$$\begin{aligned} \alpha &= q_0 + q_1\theta + q_2\theta^2 + \frac{2 + 2\theta + 2\theta^2}{3} \\ &= \left(q_0 + \frac{2}{3}\right) + \left(q_1 + \frac{2}{3}\right)\theta + \left(q_2 + \frac{2}{3}\right)\theta^2. \end{aligned}$$

Considere $A = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - 2\theta + \theta^2}{3}\right)$. Mostremos que $\mathcal{O}_{\mathbb{K}} = A$. Se $\alpha \in A$, então existem $z_0, z_1, z_2 \in \mathbb{Z}$ tais que

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\left(\frac{-2 - 2\theta + \theta^2}{3}\right) \\ &= \left(z_0 + \frac{2z_2}{3}\right) + \left(z_1 + \frac{2z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.\end{aligned}$$

Pela igualdade de polinômios, segue que

$$\begin{cases} z_0 - \frac{2z_2}{3} = q_0 + \frac{2}{3} \\ z_1 - \frac{2z_2}{3} = q_1 + \frac{2}{3} \\ \frac{z_2}{3} = q_2 + \frac{2}{3} \end{cases} \Rightarrow \begin{cases} z_0 = q_0 + 2q_2 + 2 \\ z_1 = q_1 + 2q_2 + 2 \\ z_3 = 3q_2 + 2. \end{cases}$$

Como $q_i \in \mathbb{Z}$, onde $i = 1, 2, 3$, segue que $z_i \in \mathbb{Z}$, onde $i = 1, 2, 3$. Assim, $\alpha \in A \Leftrightarrow \alpha \in \mathcal{O}_{\mathbb{K}}$, isto é, $\mathcal{O}_{\mathbb{K}} = A$.

Portanto, para $m \equiv 1 \pmod{9}$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - 2\theta + \theta^2}{3}\right)$.

• $m \equiv -1 \pmod{9}$:

1. Na linha 8, $r_0 = 1, r_1 = 2$ e $r_2 = 1$. Assim,

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + \frac{1 + 2\theta + \theta^2}{3} \\ &= \left(q_0 + \frac{1}{3}\right) + \left(q_1 + \frac{2}{3}\right)\theta + \left(q_2 + \frac{1}{3}\right)\theta^2.\end{aligned}$$

Considere $A = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - \theta + \theta^2}{3}\right)$. Mostremos que $\mathcal{O}_{\mathbb{K}} = A$. Se $\alpha \in A$, então existem $z_0, z_1, z_2 \in \mathbb{Z}$ tais que

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\left(\frac{-2 - \theta + \theta^2}{3}\right) \\ &= \left(z_0 + \frac{2z_2}{3}\right) + \left(z_1 - \frac{z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.\end{aligned}$$

Fazendo as comparações de α , segue que

$$\begin{cases} z_0 - \frac{2z_2}{3} = q_0 + \frac{1}{3} \\ z_1 - \frac{z_2}{3} = q_1 + \frac{2}{3} \\ \frac{z_2}{3} = q_2 + \frac{1}{3} \end{cases} \Rightarrow \begin{cases} z_0 = q_0 + 2q_2 + 1 \in \mathbb{Z} \\ z_1 = q_1 + 2q_2 + 1 \in \mathbb{Z} \\ z_3 = 3q_2 + 1 \in \mathbb{Z}. \end{cases}$$

Portanto, $\alpha \in A$. Assim, $\mathcal{O}_{\mathbb{K}} = A$.

2. Para a linha 11, $r_0 = 2$, $r_1 = 1$ e $r_2 = 2$. Assim,

$$\begin{aligned}\alpha &= q_0 + q_1\theta + q_2\theta^2 + \frac{2 + \theta + 2\theta^2}{3} \\ &= \left(q_0 + \frac{2}{3}\right) + \left(q_1 + \frac{1}{3}\right)\theta + \left(q_2 + \frac{2}{3}\right)\theta^2.\end{aligned}$$

Considere $A = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - \theta + \theta^2}{3}\right)$. Mostremos que $\mathcal{O}_{\mathbb{K}} = A$. Se $\alpha \in A$, então existem $z_0, z_1, z_2 \in \mathbb{Z}$ tais que

$$\begin{aligned}\alpha &= z_0 + z_1\theta + z_2\left(\frac{-2 - \theta + \theta^2}{3}\right) \\ &= \left(z_0 + \frac{2z_2}{3}\right) + \left(z_1 - \frac{z_2}{3}\right)\theta + \left(\frac{z_2}{3}\right)\theta^2.\end{aligned}$$

Fazendo as comparações de α , segue que

$$\begin{cases} z_0 - \frac{2z_2}{3} = q_0 + \frac{2}{3} \\ z_1 - \frac{z_2}{3} = q_1 + \frac{1}{3} \\ \frac{z_2}{3} = q_2 + \frac{2}{3} \end{cases} \Rightarrow \begin{cases} z_0 = q_0 + 2q_2 + 2 \in \mathbb{Z} \\ z_1 = q_1 + q_2 + 1 \in \mathbb{Z} \\ z_3 = 3q_2 + 2 \in \mathbb{Z}. \end{cases}$$

Portanto, $\alpha \in A$. E assim, $\mathcal{O}_{\mathbb{K}} = A$.

Logo, para $m \equiv -1 \pmod{9}$, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\left(\frac{-2 - \theta + \theta^2}{3}\right)$.

Portanto, concluímos a análise de todos os casos possíveis, o que prova o resultado. $\square$

Corolário 2.4.11. *Seja $\mathbb{K}$ um corpo cúbico. Seja m um inteiro livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[3]{m}$. Uma base integral de $\mathbb{K}$ é dada por*

1. Se $m \not\equiv \pm 1 \pmod{9}$, então $\{1, \theta, \theta^2\}$;
2. Se $m \equiv 1 \pmod{9}$, então $\left\{1, \theta, \frac{-2 - 2\theta + \theta^2}{3}\right\}$;
3. Se $m \equiv -1 \pmod{9}$, então $\left\{1, \theta, \frac{-2 - \theta + \theta^2}{3}\right\}$.

Demonstração. A demonstração segue direto da Definição de base integral (2.4.4) e do Teorema 2.4.10. $\square$

2.5 Discriminante

A seguir, apresentamos o conceito de discriminante. O objetivo geral é abordar o discriminante de corpos de números, mas para isso, iremos introduzir o conceito em extensão de anéis e em polinômios. Para isso, considere A e B anéis tal que B é um A -módulo finitamente gerado de posto n .

Definição 2.5.1. Sejam B um anel e A um subanel de B tal que B é um A -módulo livre finitamente gerado de posto n . Se $(x_1, \dots, x_n) \in B^n$, chamamos de **discriminante** de $(x_1, \dots, x_n)$ ao elemento de A dado por

$$D_{B/A}(x_1, \dots, x_n) = \det(\text{Tr}_{B/A}(x_i x_j)), \quad \text{onde } i, j = 1, \dots, n.$$

Observação 2.5.2. Analogamente ao traço e a norma, podemos simplesmente denotar o discriminante $D_{B/A}(\alpha_1, \dots, \alpha_n)$ por $D(\alpha_1, \dots, \alpha_n)$ quando não houver risco de confusão. No caso de corpos de números, sempre utilizamos a notação reduzida.

Proposição 2.5.3. Sejam $A \subset B$ anéis tal que B é um A -módulo livre finitamente gerado de posto n . Seja $\{\alpha_1, \dots, \alpha_n\}$ um conjunto de elementos de B tal que $\beta_i = \sum_{j=1}^n a_{ij} \alpha_j$, com $a_{ij} \in A$, para $i = 1, \dots, n$. Assim,

$$D_{B/A}(\beta_1, \dots, \beta_n) = (\det(a_{ij}))^2 D_{B/A}(\alpha_1, \dots, \alpha_n).$$

Demonstração. Por definição, segue que

$$D_{B/A}(\beta_1, \dots, \beta_n) = \det(\text{Tr}_{B/A}(\beta_r \beta_s)), \quad \text{onde } r, s = 1, \dots, n.$$

Por hipótese, segue que

$$\beta_r = \sum_{i=1}^n a_{ri} \alpha_i \text{ e } \beta_s = \sum_{j=1}^n a_{sj} \alpha_j.$$

Assim,

$$\beta_r \beta_s = \sum_{i=1}^n a_{ri} \alpha_i \sum_{j=1}^n a_{sj} \alpha_j = \sum_{i=1}^n \sum_{j=1}^n a_{ri} a_{sj} \alpha_i \alpha_j.$$

Dessa forma, $\text{Tr}_{B/A}(\beta_r \beta_s) = \sum_{i=1}^n a_{ri} a_{sj} \text{Tr}_{B/A}(\alpha_i \alpha_j)$. Colocando na forma matricial, segue que

$$(\text{Tr}_{B/A}(\beta_r \beta_s)) = (a_{ri})(\text{Tr}_{B/A}(\alpha_i \alpha_j))(a_{sj})^t.$$

Logo,

$$\begin{aligned} D_{B/A}(\beta_1, \dots, \beta_n) &= \det(\text{Tr}_{B/A}(\beta_r \beta_s)) = \det((a_{ri})(\text{Tr}_{B/A}(\alpha_i \alpha_j))(a_{sj})^t) \\ &= \det(a_{ri}) \det(\text{Tr}_{B/A}(\alpha_i \alpha_j)) \det((a_{sj})^T) \\ &= (\det(a_{ri}))^2 \det(\text{Tr}_{B/A}(\alpha_i \alpha_j)) \\ &= (\det(a_{i,j}))^2 D_{B/A}(\alpha_1, \dots, \alpha_n). \end{aligned}$$

Portanto,

$$D_{B/A}(\beta_1, \dots, \beta_n) = (\det(a_{i,j}))^2 D_{B/A}(\alpha_1, \dots, \alpha_n),$$

o que prova o resultado. $\square$

Corolário 2.5.4. Seja A um domínio. Se $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ são bases de B sobre A , então $D_{B/A}(\alpha_1, \dots, \alpha_n)$ e $D_{B/A}(\beta_1, \dots, \beta_n)$ são associados ou ambos possuem determinantes nulos.

Demonstração. Como $\{\alpha_1, \dots, \alpha_n\}$ é uma base, segue que existem elementos $a_{ij} \in A$ tais que $\beta_j = \sum_{i=1}^n a_{ij} \alpha_i$, onde $j = 1, \dots, n$, ou seja, podemos escrever cada β_j como uma combinação linear dos elementos dessa base. Assim, pela Proposição 2.5.3, segue que

$$D_{B/A}(\beta_1, \dots, \beta_n) = (\det(a_{ij}))^2 D_{B/A}(\alpha_1, \dots, \alpha_n).$$

Como (a_{ij}) é uma matriz inversível, segue que o determinante de (a_{ij}) é uma unidade do anel A . Mas, isso implica que $D_{B/A}(\alpha_1, \dots, \alpha_n)$ e $D_{B/A}(\beta_1, \dots, \beta_n)$ são elementos associados ou ambos determinantes são nulos. $\square$

Observação 2.5.5. Pela Proposição 2.5.3 e Corolário 2.5.4, se $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ são duas bases integrais de um corpo de números algébrico, então $D(\alpha_1, \dots, \alpha_n) = D(\beta_1, \dots, \beta_n)$. Ainda, se $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral de $\mathbb{K}$ e $\{\beta_1, \dots, \beta_n\} \subset \mathcal{O}_{\mathbb{K}}$ é tal que $D(\alpha_1, \dots, \alpha_n) = D(\beta_1, \dots, \beta_n)$, então $\{\beta_1, \dots, \beta_n\}$ também é uma base integral para $\mathbb{K}$.

Proposição 2.5.6. *Seja A um domínio. Se o conjunto $\{\alpha_1, \dots, \alpha_n\}$ de elementos de B é linearmente dependente sobre A , então*

$$D_{B/A}(\alpha_1, \dots, \alpha_n) = 0.$$

Demonstração. Como $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ é linearmente dependente sobre A , segue que existem $a_1, \dots, a_n \in A$, não todos nulos, tais que

$$a_1 \alpha_1 + \dots + a_n \alpha_n = 0.$$

Sem perda de generalidade, tome $a_1 \neq 0$. Considere agora o conjunto $\{\alpha'_1, \dots, \alpha'_n\}$ de elementos de B , onde $\alpha'_1 = 0$ e $\alpha'_i = \alpha_i$, para $i = 2, \dots, n$. Assim,

$$\{\alpha'_1, \alpha'_2, \dots, \alpha'_n\} = \{0, \alpha_2, \dots, \alpha_n\}.$$

Desse modo,

$$D_{B/A}(\alpha'_1, \dots, \alpha'_n) = D_{B/A}(0, \alpha_2, \dots, \alpha_n) = 0,$$

uma vez que a matriz da aplicação traço possui a primeira linha nula. Agora,

$$\begin{cases} \alpha'_1 = 0 = a_1 \alpha_1 + a_2 \alpha_2 + \dots + a_n \alpha_n \\ \alpha'_2 = \alpha_2 = 0 \alpha_1 + \alpha_2 + \dots + 0 \alpha_n \\ \alpha'_3 = \alpha_3 = 0 \alpha_1 + 0 \alpha_2 + \alpha_3 + \dots + 0 \alpha_n \\ \alpha'_n = \alpha_n = 0 \alpha_1 + \dots + 1 \alpha_n, \end{cases} \Rightarrow \begin{pmatrix} \alpha'_1 \\ \alpha'_2 \\ \vdots \\ \alpha'_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

Usando a Proposição 2.5.3, segue que

$$0 = D_{B/A}(0, \alpha_2, \dots, \alpha_n) = D_{B/A}(\alpha'_1, \dots, \alpha'_n) = (\det(a_{i,j}))^2 D_{B/A}(\alpha_1, \dots, \alpha_n),$$

onde

$$(a_{i,j}) = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Como $\det(a_{i,j}) = a_1 \neq 0$ e A é um domínio, segue que $D_{B/A}(\alpha_1, \dots, \alpha_n) = 0$. $\square$

A seguir, considere $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos de números e $\alpha_1, \dots, \alpha_n \in \mathcal{O}_{\mathbb{K}}$. O discriminante da n -upla $(\alpha_1, \dots, \alpha_n)$ é denotado por $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n)$, ou simplesmente por $D(\alpha_1, \dots, \alpha_n)$.

Definição 2.5.7. O discriminante do corpo de números $\mathbb{K}$ é definido como o discriminante de uma base integral de seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ e denotado por $d(\mathbb{K})$.

Exemplo 2.5.8. Pelo Exemplo 2.4.9, segue que o determinante de um corpo quadrático $\mathbb{Q}(\sqrt{m})$, com m livre de quadrados, é dado por

$$d(\mathbb{K}) = \begin{cases} 4m, & \text{se } m \not\equiv 1 \pmod{4} \\ m, & \text{se } m \equiv 1 \pmod{4}. \end{cases}$$

De fato: Se $m \not\equiv 1 \pmod{4}$, vimos que a base integral de $\mathbb{K}$ é $\{1, \sqrt{m}\}$. Assim,

$$d(\mathbb{K}) = D(1, \sqrt{m}) = \begin{vmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{vmatrix}^2 = (-2\sqrt{m})^2 = 4m.$$

Por outro lado, se $m \equiv 1 \pmod{4}$, então a base integral de $\mathbb{K}$ é dada por $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$, de modo que

$$d(\mathbb{K}) = D\left(1, \frac{1+\sqrt{m}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{vmatrix}^2 = (-\sqrt{m})^2 = m.$$

Corolário 2.5.9. Se $\mathbb{K}$ é um corpo quadrático real, então $\mathbb{K} = \mathbb{Q}(\sqrt{d(\mathbb{K})})$.

Demonstração. Segue do fato que $\sqrt{d(\mathbb{K})} = \sqrt{m}$ ou $2\sqrt{m}$. □

Proposição 2.5.10. Sejam o conjunto $\{\alpha_1, \dots, \alpha_n\}$ de elementos de $\mathcal{O}_{\mathbb{L}}$. Se

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) = 0,$$

então o conjunto $\{\alpha_1, \dots, \alpha_n\}$ é linearmente dependente sobre $\mathbb{K}$.

Demonstração. Suponhamos que $D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) = 0$. Da definição, segue que

$$\det(\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)) = \det \begin{pmatrix} \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_1) & \cdots & \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_n) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_1) & \cdots & \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_n) \end{pmatrix} = 0.$$

Como esse determinante é nulo, cada coluna da matriz acima são linearmente dependentes sobre $\mathbb{K}$. Chamemos cada coluna de C_i , onde $i = 1, \dots, n$. Por serem linearmente dependentes sobre $\mathbb{K}$, existem $a_1, a_2, \dots, a_n \in \mathbb{K}$, não todos nulos, tais que

$$a_1 C_1 + a_2 C_2 + \cdots + a_n C_n = 0 \Rightarrow \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot \begin{pmatrix} \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_1) & \cdots & \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_1 \alpha_n) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_1) & \cdots & \text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_n \alpha_n) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Considere $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$. Suponha que $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ é linearmente independente sobre $\mathbb{K}$. Assim, $\alpha \neq 0$. Agora, para cada $j = 1, 2, \dots, n$, segue que

$$\begin{aligned} \text{Tr}_{B/A}(\alpha\alpha_j) &= \text{Tr}_{\mathbb{L}/\mathbb{K}}(a_1\alpha_1\alpha_j + a_2\alpha_2\alpha_j + \cdots + a_n\alpha_n\alpha_j) \\ &= a_1\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_1\alpha_j) + a_2\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_2\alpha_j) + \cdots + a_n\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_n\alpha_j) = 0. \end{aligned}$$

Novamente, do fato de que $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ serem linearmente independentes sobre $\mathbb{K}$, podemos concluir que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como $\alpha \neq 0$, segue que $\{\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_n\}$ também é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, para todo $\beta \in \mathbb{L}$, segue que β é uma combinação linear dos elementos da base $\{\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_n\}$. Logo, $\text{Tr}_{\mathbb{L}/\mathbb{K}}(\beta) = 0$. Em particular, para $\beta = 1$, teríamos $\text{Tr}_{\mathbb{L}/\mathbb{K}}(1) = 0$, o que é um absurdo, pela própria definição de traço. Portanto, o conjunto $\{\alpha_1, \dots, \alpha_n\}$ é linearmente dependente sobre $\mathbb{K}$. $\square$

Lema 2.5.11. (Lema de Dedekind) *Se G é um grupo, $\mathbb{K}$ um corpo e $\sigma_1, \dots, \sigma_n$ são homomorfismos distintos e não nulos de G no grupo multiplicativo $\mathbb{K}^*$, então os σ_i 's são linearmente independentes sobre $\mathbb{K}$.*

Demonstração. Se os σ_i 's são linearmente dependentes, então existem $a_1, \dots, a_n \in \mathbb{K}$, não todos nulos, tais que $\sum_{i=1}^n a_i\sigma_i = 0$. Seja o r o menor número possível dos a_i 's não nulos. Se $r = 1$, então $a_1\sigma_1 = 0$. Mas, isso implicaria que $a_1 = 0$ ou $\sigma_1 = 0$, o que não ocorre, pois já estamos considerando os a_i 's não nulos e, claramente, os σ_i 's não nulos. Logo, $r \geq 2$. Considere $g \in G$. Assim,

$$a_1\sigma_1(g) + a_2\sigma_2(g) + \cdots + a_r\sigma_r(g) = 0. \quad (2.8)$$

Como cada σ_i é homomorfismo, segue que a Equação (2.8) é válida para todo $g \in G$. Seja $h \in G$. Para gh , segue que

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_2(h) + \cdots + a_r\sigma_r(g)\sigma_r(h) = 0. \quad (2.9)$$

Agora, vamos multiplicar $\sigma_1(h)$ na Equação (2.8) e, em seguida, subtrair da Equação (2.9), e assim,

$$\begin{aligned} \sigma_2(g)\sigma_2(h) + \cdots + a_r\sigma_r(g)\sigma_r(h) - \sigma_1(h)[a_1\sigma_1(g) + a_2\sigma_2(g) + \cdots + a_r\sigma_r(g)] &= 0 \Rightarrow \\ a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_1(h) + \cdots + a_r\sigma_r(g)\sigma_1(h) &= 0 \Rightarrow \\ a_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \cdots + a_r(\sigma_1(h) - \sigma_r(h))\sigma_r(g) &= 0. \end{aligned}$$

Como isso vale para todo $g \in G$ e tomamos r o menor possível, segue que

$$a_2(\sigma_1(h) - \sigma_2(h)) = 0 \Rightarrow a_2 = 0 \text{ ou } \sigma_1(h) - \sigma_2(h) = 0,$$

e assim, como $a_2 \neq 0$, segue que $\sigma_1(h) = \sigma_2(h)$, para todo $h \in G$. Mas, isto é um absurdo, pois, por hipótese, os σ_i 's são distintos. Portanto, podemos concluir que os σ_i 's são linearmente independentes. $\square$

Proposição 2.5.12. *Seja $\mathbb{L}$ uma extensão finita de grau n de um corpo $\mathbb{K}$, onde $\mathbb{K}$ é finito ou tem característica zero. Sejam $\sigma_1, \dots, \sigma_n$ os $\mathbb{K}$ -monomorfismos distintos de $\mathbb{L}$. Se $\{\alpha_1, \dots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração. Por definição, segue que

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)).$$

Como o traço de $\alpha_i \alpha_j$ é a soma de seus conjugados, segue que

$$\begin{aligned} D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) &= \det(\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha_i \alpha_j)) = \det\left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j)\right) \\ &= \det\left(\sum_{k=1}^n \sigma_k(\alpha_i) \sigma_k(\alpha_j)\right). \end{aligned}$$

Note que

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} = \left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j)\right),$$

ou seja,

$$(\sigma_i(\alpha_j))^2 = \left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j)\right) \Rightarrow \det(\sigma_i(\alpha_j))^2 = \det\left(\sum_{k=1}^n \sigma_k(\alpha_i \alpha_j)\right)$$

Assim,

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2,$$

o que prova o resultado. $\square$

Corolário 2.5.13. *Com as hipóteses da Proposição 2.5.12,*

$$D_{\mathbb{L}/\mathbb{K}}(\alpha_1, \dots, \alpha_n) = \det(\sigma_i(\alpha_j))^2 \neq 0.$$

Demonstração. Suponha que $\det(\sigma_i(\alpha_j)) = 0$. Assim, existem $a_1, \dots, a_n \in \mathbb{C}$, não todos nulos, tais que

$$\sum_{i=1}^n a_i (\sigma_i(\alpha_j)) = 0, \quad \text{onde } j = 1, \dots, n.$$

Pela linearidade, segue que

$$\sum_{i=1}^n a_i \sigma_i(\alpha) = 0, \quad \text{para todo } \alpha \in \mathbb{L},$$

mas isso é um absurdo, pois pelo Lema de Dedekind 2.5.11, segue que os σ_i são linearmente independentes. Logo, $\det(\sigma_i(\alpha_j))^2 \neq 0$, o que prova o corolário $\square$

Proposição 2.5.14. *Se $\mathbb{K}$ é um corpo finito ou de característica zero, $\mathbb{L} = \mathbb{K}(\alpha)$ uma extensão finita de $\mathbb{K}$ de grau n e $p(x)$ o polinômio minimal de α sobre $\mathbb{K}$, então*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(p'(\alpha)),$$

onde $p'(x)$ é a derivada de $p(x)$.

Demonstração. Sejam $\alpha_1, \alpha_2, \dots, \alpha_n$ as raízes de $p(x)$ em uma extensão de $\mathbb{K}$, que são conjugados de α . Pela Proposição 2.5.12, segue que

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}) = \det(\sigma_i(\alpha^j))^2 = \det(\alpha_i^j)^2,$$

onde $j = 0, 1, \dots, n-1$ e $\sigma_i(\alpha) = \alpha_i$, para $i = 1, 2, \dots, n$, são os $\mathbb{K}$ -monomorfismos de $\mathbb{K}(\alpha)$. Além disso, lembre que $\det(\sigma_i(\alpha^j)) = \det(\sigma_i(\alpha^j))^T$. Assim,

$$\begin{aligned} \det(\sigma_i(\alpha^j)) &= \begin{vmatrix} \sigma_1(1) & \sigma_1(\alpha) & \dots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \sigma_2(\alpha) & \dots & \sigma_2(\alpha^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(1) & \sigma_n(\alpha) & \dots & \sigma_n(\alpha^{n-1}) \end{vmatrix} = \begin{vmatrix} \sigma_1(1) & \sigma_2(1) & \dots & \sigma_n(1) \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \dots & \sigma_n(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha^{n-1}) & \sigma_2(\alpha^{n-1}) & \dots & \sigma_n(\alpha^{n-1}) \end{vmatrix} \\ &= \begin{vmatrix} 1(\alpha) & 1 & \dots & 1 \\ \sigma_1(\alpha) & \sigma_2(\alpha) & \dots & \sigma_n(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha)^{n-1} & \sigma_2(\alpha)^{n-1} & \dots & \sigma_n(\alpha)^{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{vmatrix}. \end{aligned}$$

Note que este determinante é de Vandermonde. Logo,

$$\det(\sigma_i(\alpha^j)) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j),$$

e assim,

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Por outro lado, o polinômio minimal de α é dado por

$$p(x) = D_{i=1}^n (x - \alpha_i) = (x - \alpha)g(x),$$

onde $g(x) = D_{i=1}^n (x - \alpha_i)$. Daí,

$$p'(x) = \sum_{j=1}^n D_{i=1, i \neq j}^n (x - \alpha_i) \quad \text{e} \quad p'(\alpha_j) = D_{i=1, i \neq j}^n (\alpha_j - \alpha_i),$$

e assim,

$$D_{j=1}^n p'(\alpha_j) = D_{i,j=1, i \neq j}^n (\alpha_j - \alpha_i).$$

Note que $D_{j=1}^n p'(\alpha_j) = N_{\mathbb{L}/\mathbb{K}}(p'(\alpha))$. Logo,

$$N_{\mathbb{L}/\mathbb{K}}(p'(\alpha)) = \prod_{\substack{i,j=1, \\ i \neq j}}^n (\alpha_j - \alpha_i). \quad (2.10)$$

Agora, em $\prod_{\substack{i,j=1, \\ i \neq j}}^n (\alpha_j - \alpha_i)$ cada fator $(\alpha_i - \alpha_j)$, para $i < j$, aparece duas vezes, uma como

$(\alpha_i - \alpha_j)$ e outra como $(\alpha_j - \alpha_i)$. Daí,

$$(\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = -(\alpha_i - \alpha_j)^2 = (-1)(\alpha_i - \alpha_j).$$

Desse modo, na Equação (2.10), aparece o termo $(-1)^s$, onde s é o número de pares (i, j) , com $1 \leq i < j \leq n$, ou seja,

$$N_{\mathbb{L}/\mathbb{K}}(p'(\alpha)) = \prod_{1 \leq i < j \leq n} (-1)^s (\alpha_i - \alpha_j)^2.$$

Mas,

- Se $i = 1$, então $j = 2, 3, \dots, n$ e $s = 1$;
- Se $i = 2$, então $j = 3, \dots, n$ e $s = 2$;
- $\vdots$
- Se $i = n - 1$, então $j = n$ e $s = n - 1$.

Assim,

$$(n-1) + (n-2) + \dots + 1 = \frac{((n-1)+1)n-1}{2} = \frac{1}{2}n(n-1) = s.$$

Logo,

$$N_{\mathbb{L}/\mathbb{K}}(p'(\alpha)) = (-1)^{\frac{1}{2}n(n-1)} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{1}{2}n(n-1)} D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}),$$

e assim,

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(p'(\alpha)),$$

como queríamos. □

Exemplo 2.5.15. Considere um corpo cúbico puro $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta = \sqrt[3]{m}$. Este corpo $\mathbb{K}$ possui uma base potente dada por $\{1, \theta, \theta^2\}$ e, assim, satisfaz a Proposição 2.5.14.

Corolário 2.5.16. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n . Se o polinômio minimal de θ é $p(x) = x^n + ax + b \in \mathbb{Z}[x]$, com a e b não nulos, então*

$$D(1, \theta, \theta^2, \dots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} [n^n b^{n-1} + (-1)^{n+1} (n-1)^{n-1} a^n].$$

Demonstração. Sejam $p(x) = x^n + ax + b \in \mathbb{K}[x]$ e α uma raiz de $p(x)$. Assim, $p'(\alpha) = n\alpha^{n-1} + a$. Agora, se $p(\alpha) = 0$, então

$$\alpha^n + a\alpha + b = 0.$$

Logo,

$$\alpha^n = -a\alpha - b \stackrel{(\alpha^{-1})}{\Rightarrow} (\alpha^n)\alpha^{-1} = (-a\alpha - b)\alpha,$$

e assim,

$$\alpha^{n-1} = -a\alpha\alpha^{-1} - b\alpha^{-1} \Rightarrow \alpha^{n-1} = -a - b\alpha^{-1} \stackrel{(\cdot n)}{\Rightarrow} n\alpha^{n-1} = -na - nb\alpha^{-1}.$$

Logo,

$$p'(\alpha) = n\alpha^{n-1} + a = (-na - nb\alpha^{-1}) + a = -na + a - nb\alpha^{-1} = -(n-1)a - nb\alpha^{-1}.$$

Assim,

$$\begin{aligned} p'(\alpha) &= -(n-1)a - (nb)\alpha^{-1} \Rightarrow p'(\alpha) + (n-1)a = -(nb)\alpha^{-1} \\ \Rightarrow \alpha^{-1} &= \frac{p'(\alpha) + (n-1)a}{-(nb)} \Rightarrow \alpha^{-1} = (-nb)^{-1}(p'(\alpha) + (n-1)a) \\ \Rightarrow (\alpha^{-1})^{-1} &= [(-nb)^{-1}(p'(\alpha) + (n-1)a)]^{-1} \\ \Rightarrow \alpha &= (-nb)[p'(\alpha) + (n-1)a]^{-1}. \end{aligned}$$

Aplicando a p , segue que

$$\begin{aligned}
 p(\alpha) &= p((-nb)[p'(\alpha) + (n-1)a]^{-1}) \\
 \xRightarrow{p(\alpha)=0} 0 &= (-nb(p'(\alpha) + (n-1)a)^{-1})^n + a(-nb(p'(\alpha) + (n-1)a)^{-1}) + b \\
 &\Rightarrow (-nb)^n[(p'(\alpha) + (n-1)a)^{-n}] + (-anb)[p'(\alpha) + (n-1)a]^{-1} + b = 0 \\
 &\Rightarrow \frac{(-nb)^n}{((p'(\alpha) + (n-1)a))^n} - \frac{nab}{((p'(\alpha) + (n-1)a))} + b = 0 \\
 &\Rightarrow \frac{(-nb)^n - nab((p'(\alpha) + (n-1)a))^{n-1} + b((p'(\alpha) + (n-1)a))^n}{((p'(\alpha) + (n-1)a))^n} = 0.
 \end{aligned}$$

Note que $((p'(\alpha) + (n-1)a))^n \neq 0$. Assim,

$$\begin{aligned}
 (-nb)^n - nab((p'(\alpha) + (n-1)a))^{n-1} + b((p'(\alpha) + (n-1)a))^n &= 0 \xRightarrow{(b^{-1})} \\
 ((p'(\alpha) + (n-1)a))^n - na((p'(\alpha) + (n-1)a))^{n-1} + (-1)^n n^n b^{n-1} &= 0.
 \end{aligned}$$

Assim, o polinômio minimal de $p'(\alpha)$ sobre $\mathbb{K}$ é dado por

$$q(x) = (x + (n-1)a)^n - na(x + (n-1)a)^{n-1} + (-1)^n b^{n-1} n^n.$$

O termo constante de $q(x)$ é dado por

$$\begin{aligned}
 b_0 &= (n-1)^n a^n - na(n-1)^{n-1} a^{n-1} + (-1)^n n^n b^{n-1} \\
 &= (n-1)^{n-1} a^n - na(n-1)^{n-1} a^{n-1} + (-1)^n n^n b^{n-1} \\
 &= [(n-1)^n - n(n-1)^{n-1}] a^n + (-1)^n n^n b^{n-1} \\
 &= (-1)(n-1)^n a^n + (-1)^n n^n b^{n-1}.
 \end{aligned}$$

Como a norma de $p'(\alpha)$ é $(-1)^n$ vezes o termo constante do polinômio $q(x)$, segue que

$$N_{\mathbb{K}}(p'(\alpha)) = (-1)^n b = n^n b^{n-1} + (-1)^{n+1} (n-1)^{n-1} a^n.$$

Pela Proposição 2.5.14, segue que

$$\begin{aligned}
 D(1, \theta, \theta^2, \dots, \theta^{n-1}) &= (-1)^{\frac{n(n-1)}{2}} (N(p'(\theta))) \\
 &= (-1)^{\frac{n(n-1)}{2}} [n^n b^{n-1} + (-1)^{n+1} (n-1)^{n-1} a^n],
 \end{aligned}$$

o que prova o corolário. □

Corolário 2.5.17. *Seja $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo de números de grau n . Se o polinômio minimal de θ é $p(x) = x^n - m \in \mathbb{Z}[x]$, com m não nulo, então*

$$D(1, \theta, \theta^2, \dots, \theta^{n-1}) = (-1)^{\frac{n^2+n+2}{2}} [n^n m^{n-1}].$$

Demonstração. Seja $p(x) = x^n - m$ o polinômio minimal de θ . Assim, $p'(x) = nx^{n-1} \Rightarrow p'(\theta) = n\theta^{n-1}$. Por outro lado,

$$p(\theta) = \theta^n - m = 0 \Leftrightarrow \theta^n = m \Leftrightarrow n\theta^{n-1} = nm\theta^{-1}.$$

Assim,

$$p'(\theta) = nm\theta^{-1} \Leftrightarrow \theta^{-1} = (nm)^{-1}(p'(\theta)) \Leftrightarrow \theta = \frac{nm}{p'(\theta)}.$$

Como $p(\theta) = 0$, segue que $\left(\frac{nm}{p'(\theta)}\right)^n - m = 0$. Dessa forma,

$$\frac{(nm)^n}{(p'(\theta))^n} - m = 0 \Leftrightarrow \frac{(nm)^n - m(p'(\theta))^n}{(p'(\theta))^n} = 0.$$

Como $(p'(\theta)) \neq 0$, segue que

$$(nm)^n - m(p'(\theta))^n = 0 \stackrel{(\cdot m^{-1})}{\Leftrightarrow} (p'(\theta))^n n^n m^{n-1} = 0.$$

Assim, o polinômio minimal de $p'(\theta)$ sobre $\mathbb{Q}$ é dado por $g(x) = x^n - n^n m^{n-1}$. Denote por $k = -n^n m^{n-1}$ o termo constante de g . Como a norma de $p'(\theta)$ é $(-1)^n$ -vezes o termo constante de g , segue que

$$\begin{aligned} N(p'(\theta)) &= (-1)^n k \\ &= (-1)^n - n^n m^{n-1} \\ &= (-1)^{n-1} nm^{n-1}. \end{aligned}$$

Pela Proposição 2.5.14, segue que

$$\begin{aligned} D(1, \theta, \theta^2, \dots, \theta^{n-1}) &= (-1)^{\frac{n(n-1)}{2}} (N(p'(\theta))) \\ &= (-1)^{\frac{n(n-1)}{2}} [(-1)^{n-1} nm^{n-1}] \\ &= (-1)^{\frac{n^2+n+2}{2}} [n^n m^{n-1}], \end{aligned}$$

o que prova o corolário. $\square$

Exemplo 2.5.18. Seja $K = \mathbb{Q}(\sqrt[3]{2})$. O polinômio minimal de $\mathbb{K}$ é dado por $x^3 - 2 \in \mathbb{Z}[x]$. Assim, pelo Corolário 2.5.17, segue que

$$D(1, \theta, \theta^2) = (-1)^{\frac{3^2+3+2}{2}} [3^3 2^{2-1}] = -27(2^2) = -128.$$

Exemplo 2.5.19. Seja $K = \mathbb{Q}(\sqrt[3]{3})$. O polinômio minimal de $\mathbb{K}$ é dado por $x^3 - 3 \in \mathbb{Z}[x]$. Assim, pelo Corolário 2.5.17, segue que

$$D(1, \theta, \theta^2) = (-1)^{\frac{3^2+3+2}{2}} [3^3 3^{2-1}] = -27(3^2) = -243.$$

Proposição 2.5.20. *Sejam $\mathbb{K}$ um corpo de números de grau n , $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ contida no anel $\mathcal{O}_{\mathbb{K}}$ de inteiros de $\mathbb{K}$. Se o discriminante $D_{\mathbb{K}}(\alpha_1, \alpha_2, \dots, \alpha_n)$ é livre de quadrados, então $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$.*

Demonstração. Considere $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. Desse modo, como $\{\alpha_1, \dots, \alpha_n\} \in \mathcal{O}_{\mathbb{K}}$, segue que

$$\alpha_j = \sum_{i=1}^n a_{ij} e_j, \text{ com } a_{ij} \in \mathbb{Z}.$$

Pela Proposição 2.5.3, segue que

$$D_{\mathbb{K}}(\alpha_1, \alpha_2, \dots, \alpha_n) = (\det(a_{ij}))^2 D_{\mathbb{K}}(e_1, e_2, \dots, e_n).$$

Como, por hipótese, $D_{\mathbb{K}}(\alpha_1, \alpha_2, \dots, \alpha_n)$ é livre de quadrados, segue que $\det(a_{ij}) = \pm 1$. Mas, isso implica que

$$\begin{aligned} D_{\mathbb{K}}(\alpha_1, \alpha_2, \dots, \alpha_n) &= (\pm 1)^2 \cdot D_{\mathbb{K}}(e_1, e_2, \dots, e_n) \Rightarrow \\ D_{\mathbb{K}}(\alpha_1, \alpha_2, \dots, \alpha_n) &= D_{\mathbb{K}}(e_1, e_2, \dots, e_n) \end{aligned}$$

E portanto, $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ também é uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$. $\square$

Proposição 2.5.21. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\alpha_1, \dots, \alpha_n \in \mathcal{O}_{\mathbb{K}}$. Se $D(\alpha_1, \dots, \alpha_n) \neq 0$, então*

$$|d(\mathbb{K})| \leq |D(\alpha_1, \dots, \alpha_n)|.$$

Além disso, se $D(\alpha_1, \dots, \alpha_n)$ é livre de quadrados, então $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral para $\mathbb{K}$.

Demonstração. Seja $\{\lambda_1, \dots, \lambda_n\}$ uma base integral para $\mathbb{K}$. Assim, existem $c_{ij} \in \mathbb{Z}$, para $i, j = 1, \dots, n$, tais que

$$\begin{cases} \alpha_1 = c_{11}\lambda_1 + c_{12}\lambda_2 + \dots + c_{1n}\lambda_n \\ \alpha_2 = c_{21}\lambda_1 + c_{22}\lambda_2 + \dots + c_{2n}\lambda_n \\ \vdots \\ \alpha_n = c_{n1}\lambda_1 + c_{n2}\lambda_2 + \dots + c_{nn}\lambda_n. \end{cases}$$

Assim,

$$D(\alpha_1, \dots, \alpha_n) = \det(c_{ij})^2 \cdot D(\lambda_1, \dots, \lambda_n) = \det(c_{ij})^2 \cdot d(\mathbb{K}) \neq 0 \Rightarrow \det(c_{ij}) \neq 0.$$

Como $\det(c_{ij}) \in \mathbb{Z}$, segue que $\det(c_{ij})^2 \geq 1$ e, assim

$$|D(\alpha_1, \dots, \alpha_n)| \geq |d(\mathbb{K})|.$$

Se $D(\alpha_1, \dots, \alpha_n)$ é livre de quadrados, então

$$\det(c_{ij}) = \pm 1 \Rightarrow D(\alpha_1, \dots, \alpha_n) = d(\mathbb{K}),$$

ou seja, $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral para $\mathbb{K}$. $\square$

Por fim, apresentamos a definição e resultados de discriminante de polinômios.

Definição 2.5.22. Sejam $\mathbb{K}$ um corpo e $f(x) = a_0 + a_1x + \dots + a_nx^n \in \mathbb{K}[x]$ um polinômio de grau n com raízes $\alpha_1, \dots, \alpha_n$. O **discriminante de $f(x)$** , denotado como $D(f)$, é definido por

$$D(f) = a_n^{2n-2} \prod_{i < j} (\alpha_j - \alpha_i)^2.$$

Se $\delta = \prod_{1 \leq i, j \leq n} (\alpha_i - \alpha_j)$, então $\delta = \det(A)$, onde

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix}.$$

Assim, $\delta^2 = \det(A) \det(A^T)$. Ainda,

$$D(f) = a_n^{2n-2}(\delta)^2 \Rightarrow D(f) = a_n^{2n-2} \det(B),$$

onde B é dada por

$$B = \begin{pmatrix} n & \alpha_1 + \dots + \alpha_n & \dots & \alpha_n^{n-1} + \dots + \alpha_n^{n-1} \\ \alpha_1 + \dots + \alpha_n & \alpha_1^2 + \dots + \alpha_n^2 & \dots & \alpha_n^n + \dots + \alpha_n^n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n^{n-1} + \dots + \alpha_n^{n-1} & \alpha_n^n + \dots + \alpha_n^n & \dots & \alpha_n^{2n-2} + \dots + \alpha_n^{2n-2} \end{pmatrix}.$$

Finalmente, se $f(x) = a_n g(x)$, onde $g(x) = \frac{a_0}{a_n} + \frac{a_1}{a_n}x + \dots + \frac{a_{n-1}}{a_n}x^{n-1} + x^n \in \mathbb{K}[x]$, então $D(f) = a_n^{2n-2} D(g)$.

Podemos, ainda, reescrever a definição do determinante de polinômios (Definição 2.5.22) da seguinte forma.

Definição 2.5.23. Seja $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{K}[x]$. O **discriminante** de $f(x)$ também pode ser definido da seguinte maneira

$$D(f) = (-1)^{\frac{1}{2}n(n-1)} \frac{1}{a_n} \det(M), \quad (2.11)$$

onde M é uma matriz $(2n-1) \times (2n-1)$ dada por

$$\begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_0 \\ na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & 1a_1 & 0 & \dots & \dots & 0 \\ 0 & na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & 1a_1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & na_n & (n-1)a_{n-1} & (n-2)a_{n-2} & \dots & 1a_1 \end{pmatrix},$$

onde as entradas são em função dos coeficientes de $f(x)$.

Exemplo 2.5.24. Se $f(x) = a_2x^2 + a_1x + a_0$, então

$$D(f) = (-1)^{\frac{2(2-1)}{2}} \frac{1}{a_2} \det \begin{pmatrix} a_2 & a_1 & a_0 \\ 2a_2 & a_1 & 0 \\ 0 & 2a_2 & a_1 \end{pmatrix} = a_1^2 - 4a_0a_2.$$

Exemplo 2.5.25. Se $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$, então

$$\begin{aligned} D(f) &= (-1)^{\frac{1}{2}3(3-1)} \frac{1}{a_3} \det \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ 3a_3 & 2a_2 & a_1 & 0 & 0 \\ 0 & 3a_3 & 2a_2 & a_1 & 0 \\ 0 & 0 & 3a_3 & 2a_2 & a_1 \end{pmatrix} \\ &= 18a_0a_1a_2a_3 - 4a_0a_2^3 + a_1^2a_2^2 - 4a_1^3a_3 - 27a_0^2a_3^2. \end{aligned}$$

Em particular, se $f(x) = x^3 + ax + b$, então $D(f) = -4a^3 - 27b^2$.

2.6 Unidades

Nesta seção, vamos relembrar definições e propriedades básicas sobre unidades em domínios de integridade.

Definição 2.6.1. Um **domínio de integridade**, ou simplesmente **domínio**, é um anel comutativo que tem uma identidade multiplicativa mas não tem divisores de zero. Um domínio D é dito corpo se para cada $a \in D$, $a \neq 0$, existe $b \in D$ tal que $ab = 1$.

Sejam $a, b, c \in D$, onde D é um domínio. Valem as seguintes propriedades:

1. $a|a$ (reflexiva);
2. $a|b$ e $b|c$ implica $a|c$ (transitiva);
3. $a|b$ e $a|c$ implica $a|xb + yc$, para quaisquer $x, y \in D$;
4. $a|b$ implica $ac|bc$;
5. $ac|bc$ e $c \neq 0$ implica $a|b$;
6. $a|0$;
7. $0|a$ implica $a = 0$.

Definição 2.6.2. Um elemento de um domínio D é chamado de **unidade** se $a|1$. O conjunto das unidades é denotado por $U(D)$ ou por D^* .

Algumas propriedades diretas das unidades são as seguintes:

1. $\pm 1 \in U(D)$;
2. Se $a \in U(D)$, então $-a \in U(D)$;
3. Se $a \in U(D)$ e $b \in U(D)$, então $ab \in U(D)$;
4. Se $a \in U(D)$, então $\pm a^n \in U(D)$, para qualquer $n \in \mathbb{Z}$.

Teorema 2.6.3. Se D é um domínio, então $U(D)$ é um grupo abeliano com respeito a multiplicação.

Demonstração. Segue da propriedade 4 que $U(D)$ é fechado sob a multiplicação. Além disso, a multiplicação de elementos de $U(D)$ são tanto comutativas quanto associativas, uma vez que D é domínio. Além disso, pela propriedade 1, o elemento 1 do anel é o elemento neutro de $U(D)$. Por fim, todo elemento de $U(D)$ tem inverso multiplicativo pela propriedade 3. Portanto, $U(D)$ é um grupo abeliano com respeito a multiplicação. $\square$

Definição 2.6.4. Sejam D um domínio e $a, b \in D$ não nulos. Os elementos a e b são ditos **elementos associados**, se um divide o outro. Se a e b são associados, denotamos $a \sim b$. Caso contrário, $a \not\sim b$.

Sobre os elementos associados, seguem as seguintes propriedades. Sejam $a, b, c \in D \setminus 0$, com D domínio. Logo,

1. $a \sim a$;

2. $a \sim b$ e $b \sim c$ implica $a \sim c$;
3. $a \sim b$ e $a \sim c$ implica $a \sim xb + yc$, para quaisquer $x, y \in D$;
4. $a \sim b$ se, e só se, $ab^{-1} \in U(D)$;
5. $ac|bc$ e $c \neq 0$ implica $a|b$;
6. $a \sim 1$ se, e só, se a é uma unidade.

Note que as propriedades 1, 2 e 3 garantem que $\sim$ é uma relação de equivalência. A classe de equivalência contendo $a \in D$ é o conjunto $\{ua \mid u \in U(D)\}$.

Exemplo 2.6.5. Em $\mathbb{Z}$, $a \sim b$ se, e somente se, $a = \pm b$, isto é, $|a| = |b|$.

Tendo lembrado estes conceitos, vamos provar um Teorema sobre unidades que será útil em demonstrações dos próximos capítulos. Note que abaixo já estamos considerando um corpo $\mathbb{K}$ e não mais apenas um domínio de integridade.

Proposição 2.6.6. *Seja $\mathbb{K}$ um corpo de números e seja $\alpha \in \mathbb{K}$. Assim, α é uma unidade de $\mathbb{K}$ se, e somente se, α é um inteiro de $\mathbb{K}$ de norma $|N(\alpha)| = \pm 1$.*

Demonstração. Se $\alpha \in U(\mathcal{O}_{\mathbb{K}})$, então $N(\alpha)$ e $N(\alpha^{-1})$ pertencem a $\mathbb{Z}$. Assim,

$$\underbrace{N(\alpha)}_{\in \mathbb{Z}} \cdot \underbrace{N(\alpha^{-1})}_{\in \mathbb{Z}} = N(\alpha\alpha^{-1}) = N(1) = 1 \Rightarrow N(\alpha) = \pm 1.$$

Por outro lado, tome α um elemento inteiro de $\mathbb{K}$ tal que $N(\alpha) = \pm 1$. Assim, existem $a_i \in \mathbb{Z}$, para $i = 1, \dots, n$, tais que

$$\begin{aligned} \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha \pm 1 &= 0 \\ \Rightarrow \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha &= \pm 1 \\ \Rightarrow \alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1) &= \pm 1 \\ \Rightarrow \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1 &= \pm\alpha^{-1} \\ \Rightarrow \pm(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1) &= \alpha^{-1}. \end{aligned}$$

Como α é inteiro, segue que α^{-1} também é inteiro. Portanto, α é uma unidade, uma vez que $\alpha\alpha^{-1} = 1$. $\square$

3 Unidades em corpos quadráticos

O objetivo deste capítulo é determinar qual o grupo das unidades de corpos quadráticos. Na Seção 3.1, apresentamos o Teorema 3.1.1, que determina o grupo de unidades $U(\mathcal{O}_{\mathbb{K}})$ para um corpo quadrático imaginário arbitrário $\mathbb{K}$.

Para determinar a estrutura do grupo de unidades $U(\mathcal{O}_{\mathbb{K}})$ de corpos quadráticos reais, o trabalho não é tão simples. Isso é feito provando que existe uma unidade η em $\mathcal{O}_{\mathbb{K}}$ tal que qualquer outra unidade do anel de inteiros é da forma $\pm\eta^n$, $n \in \mathbb{Z}$. Mais ainda, mostramos que existe uma única unidade de $\mathcal{O}_{\mathbb{K}}$ maior do que 1 com essa propriedade. Essa unidade é dita unidade fundamental de $\mathcal{O}_{\mathbb{K}}$ (ou de $\mathbb{K}$). Na Seção 3.2 será calculado o grupo das unidades do corpo quadrático real $\mathbb{Q}(\sqrt{2})$. 3.3. Nas Seções 3.4 e 3.5, abordamos as unidades de norma 1 e -1, respectivamente. A seguir, na Seção 3.6, abordamos os resultados sobre unidades em corpos quadráticos reais e, em particular, definiremos o importante conceito de unidade fundamental.

Por fim, na última seção deste capítulo, Seção 3.7, faremos uso de frações contínuas para determinar a unidade fundamental do anel de inteiros de um corpo $\mathbb{K}$.

3.1 Unidades de corpos quadráticos imaginários

O corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, com m livre de quadrado, é dito real se $\mathbb{K} \subset \mathbb{R}$ e imaginário se $\mathbb{K} \subset \mathbb{C}$. Claramente, $\mathbb{K}$ é real se $m > 0$ e imaginário se $m < 0$. A seguir, vamos determinar o conjunto de unidades $U(\mathcal{O}_{\mathbb{K}})$ para um corpo quadrático imaginário $\mathbb{K}$.

Teorema 3.1.1. *Seja $\mathbb{K}$ um corpo quadrático imaginário, ou seja, $\mathbb{K} = \mathbb{Q}(\sqrt{-m})$, com $m \in \mathbb{Z}_+$ livre de quadrados. O grupo de unidades de $\mathbb{K}$ é dado por*

$$U(\mathcal{O}_{\mathbb{K}}) = \begin{cases} \{\pm 1, \pm i\} \simeq \mathbb{Z}_4, & \text{se } m = 1; \\ \{\pm 1, \pm \omega, \pm \omega^2\} \simeq \mathbb{Z}_6, & \text{se } m = 3; \\ \{\pm 1\} \simeq \mathbb{Z}_2, & \text{nos demais casos.} \end{cases}$$

com $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$.

Demonstração. Usamos o fato de que

$$\alpha \in U(\mathcal{O}_{\mathbb{K}}) \Leftrightarrow \alpha \in \mathcal{O}_{\mathbb{K}} \text{ e } \|\alpha\| = 1.$$

Analizamos as possibilidades.

1. Se $m = 1$, então $\mathbb{K} = \mathbb{Q}(\sqrt{-1})$ e, pelo Teorema (5.4.2), segue que

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}(\sqrt{-1}) = \mathbb{Z}[i].$$

Seja $\alpha \in \mathbb{Z} + \mathbb{Z}[i]$. Logo, $\alpha = a + bi$, com $a, b \in \mathbb{Z}$. Assim,

$$\begin{aligned} \alpha \in U(\mathcal{O}_{\mathbb{K}}) &\Leftrightarrow \|\alpha\| = 1 \Leftrightarrow \sqrt{a^2 + b^2} = 1 \Leftrightarrow a^2 + b^2 = 1 \\ &\Leftrightarrow \begin{cases} a^2 = 1 \text{ e } b^2 = 0 \text{ ou} \\ a^2 = 0 \text{ e } b^2 = 1. \end{cases} \Leftrightarrow \begin{cases} a = \pm 1, b = 0 \text{ ou} \\ a = 0, b = \pm 1. \end{cases} \end{aligned}$$

Portanto, $\alpha = \pm 1$ ou $\alpha = \pm i$. Logo, para $m = 1$, $U(\mathcal{O}_{\mathbb{K}}) = \{\pm 1, \pm i\}$.

2. Se $m = 3$, então $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ e, pelo Teorema (5.4.2), segue que

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\left(\frac{1 + \sqrt{-3}}{2}\right).$$

Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$. Assim, $\alpha = a + b\left(\frac{1 + \sqrt{-3}}{2}\right) = \left(a + \frac{b}{2}\right) + i\left(\frac{b\sqrt{3}}{2}\right)$, $a, b \in \mathbb{Z}$. Logo,

$$\begin{aligned} \alpha \in U(\mathcal{O}_{\mathbb{K}}) &\Leftrightarrow \|\alpha\| = 1 \Leftrightarrow \sqrt{\left(a + \frac{b}{2}\right)^2 + \left(\frac{b\sqrt{3}}{2}\right)^2} = 1 \\ &\Leftrightarrow \frac{(2a + b)^2}{4} + \frac{3b^2}{4} = 1 \Leftrightarrow (2a + b)^2 + 3b^2 = 4. \end{aligned}$$

Agora,

- (a) $b = 0 \Rightarrow (2a)^2 = 4 \Rightarrow a^2 = 1 \Rightarrow a = \pm 1$.
- (b) $b = 1 \Rightarrow 4a^2 + 2a + 1 + 3 = 4 \Rightarrow 4a^2 + 2a = 0 \Rightarrow 2a(2a + 1) = 0 \xrightarrow{a \in \mathbb{Z}_+} a = 0$.
- (c) $b = -1 \Rightarrow 4a^2 - 2a = 0 \Rightarrow 2a(a^2 - 1) \Rightarrow a = 0$.
- (d) $b \geq 2$ não ocorre, pois não há nenhuma possibilidade que satisfaça a equação.

Substituindo os casos acima, segue que $\alpha = \pm 1$, $\alpha = \pm \omega$ ou $\alpha = \pm \omega^2$. Logo, $U(\mathcal{O}_{\mathbb{K}}) = \{\pm 1, \pm \omega, \pm \omega^2\}$.

3. Se $m = 2$ ou $m > 3$, então obtemos novamente duas opções:

- Suponha $m \not\equiv 1 \pmod{4}$. Assim, $\mathbb{K} = \mathbb{Q}(\sqrt{-m})$ tem o anel de inteiros

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}(\sqrt{-1}).$$

Agora, se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $\alpha = a + b\sqrt{-1}$, $a, b \in \mathbb{Z}$. Daí,

$$\alpha \in U(\mathcal{O}_{\mathbb{K}}) \Leftrightarrow \|\alpha\| = 1 \Leftrightarrow a^2 + b^2 m = 1.$$

Como $m \geq 2$, então devemos ter $b = 0$. Logo, $a = \pm 1$.

- Suponha $m \equiv 1 \pmod{3}$. Assim, $\mathbb{K} = \mathbb{Q}(\sqrt{-m})$ tem o anel de inteiros

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z} \left(\frac{1 + \sqrt{-m}}{2} \right).$$

$$\alpha \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \alpha = a + b \left(\frac{1 + \sqrt{-m}}{2} \right) = \left(a + \frac{b}{2} \right) + \left(\frac{b\sqrt{-m}}{2} \right).$$

Assim,

$$\alpha \in U(\mathcal{O}_{\mathbb{K}}) \Leftrightarrow \|\alpha\| = 1 \Leftrightarrow \underbrace{(2a+b)^2}_{>0} + \underbrace{mb^2}_{\geq 2} = 4.$$

Como $m > 3$, segue que $nb = 0$ e, assim, $a = \pm 1$. Dessa forma, $\alpha = \pm 1$.

Portanto, determinamos o grupo de unidades de $\mathbb{Q}(\sqrt{-m})$, com $m \in \mathbb{Z}_+$ livre de quadrados. $\square$

3.2 Unidades de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{2})$

Como veremos, não é um trabalho tão simples determinar qual o grupo de unidades de um corpo quadrático real arbitrário quanto é para corpos imaginários. Primeiro analisemos um caso particular. Para ilustrar algumas das ideias envolvidas, começamos determinando

$$U(\mathcal{O}_{\mathbb{Q}(\sqrt{2})}).$$

Teorema 3.2.1. *As unidades de $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ são dadas por $\pm(1 + \sqrt{2})^n$, com $n \in \mathbb{N}$, de modo que*

$$U(\mathbb{Z} + \mathbb{Z}\sqrt{2}) \simeq \mathbb{Z}_2 \times \mathbb{Z}.$$

Demonstração. Começamos mostrando que não existe uma unidade λ de $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ satisfazendo

$$1 < \lambda < 1 + \sqrt{2}. \quad (3.1)$$

Para isso, suponha que existe uma unidade λ que satisfaça a Equação (3.1). Pelo Teorema 2.2.25, segue que existe exatamente dois monomorfismos σ_1 e $\sigma_2 : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{C}$, dados por,

$$\begin{cases} \sigma_1(x + y\sqrt{2}) = x + y\sqrt{2}, \\ \sigma_2(x + y\sqrt{2}) = x - y\sqrt{2}, \end{cases}$$

para $x, y \in \mathbb{Q}$. Como, por hipótese, λ é unidade, segue que $\lambda|1$. Dessa forma,

$$1 = \lambda \cdot \mu, \text{ para algum } \mu \in (\mathbb{Z} + \mathbb{Z}\sqrt{2}). \quad (3.2)$$

Seja $\lambda' = \sigma_2(\lambda)$ e $\mu' = \sigma_2(\mu)$. Aplicando σ_2 na Equação (3.2), segue que

$$1 = \lambda\mu \Rightarrow \sigma_2(1) = \sigma(\lambda\mu) \Rightarrow 1 = \sigma_2(\lambda)\sigma_2(\mu) \Rightarrow 1 = \lambda'\mu'.$$

Assim,

$$1 = 1.1 = (\lambda\mu)(\lambda'\mu') = (\lambda\lambda')(\mu\mu').$$

Agora, note que $\lambda\lambda' \in \mathbb{Z}$ e $\mu\mu' \in \mathbb{Z}$. Assim, novamente de λ ser uma unidade, segue que

$$\lambda\lambda' = \pm 1.$$

Vamos analisar essas duas possibilidades:

1. $\lambda\lambda' = 1$: Pela desigualdade (3.1), segue que

$$1 < \lambda < 1 + \sqrt{2} \Rightarrow \frac{1}{1} > \frac{1}{\lambda} > \frac{1}{1 + \sqrt{2}}.$$

Como $\lambda' = \frac{1}{\lambda}$, segue que

$$1 > \lambda' > \frac{1}{1 + \sqrt{2}} = \frac{1}{1 + \sqrt{2}} \cdot \frac{1 - \sqrt{2}}{1 - \sqrt{2}} = \frac{1 - \sqrt{2}}{1^2 - (\sqrt{2})^2} = \frac{1 - \sqrt{2}}{-1} = \sqrt{2} - 1.$$

Assim,

$$\sqrt{2} - 1 = \frac{1}{1 + \sqrt{2}} < \lambda' < 1. \quad (3.3)$$

Somando as Equações (3.1) e (3.3), segue que

$$1 + (\sqrt{2} - 1) < \lambda + \lambda' < 1 + (\sqrt{2} + 1) \Leftrightarrow \sqrt{2} < \lambda + \lambda' < 1 + \sqrt{2}$$

se, e somente se,

$$\frac{\sqrt{2}}{2} < \frac{\lambda + \lambda'}{2} < \frac{2 + \sqrt{2}}{2} \Leftrightarrow 0.7 < \frac{\sqrt{2}}{2} < \frac{\lambda\lambda'}{2} < \frac{2 + \sqrt{2}}{2} = 1 + \frac{\sqrt{2}}{2} < 1.8,$$

uma vez que $\frac{\sqrt{2}}{2} \approx 0.707106$. Agora, como $\frac{\lambda + \lambda'}{2} \in \mathbb{Z}$, segue que $\frac{\lambda + \lambda'}{2} = 1$.

Agora, como $\lambda\lambda' = 1$ e $\frac{\lambda + \lambda'}{2} = 1$, segue que $\lambda = \lambda' = 1$. Mas, pela Equação (3.1), segue que $\lambda > 1$, o que é um absurdo. Portanto, $\lambda\lambda' \neq 1$.

2. $\lambda\lambda' = -1$. Pela Equação (3.1), segue que

$$1 < \lambda < 1 + \sqrt{2} \Rightarrow \frac{1}{\sqrt{2}} > \frac{1}{\lambda} > \frac{1}{1 + \sqrt{2}}.$$

Multiplicando em ambos os lados por -1 , segue que

$$-1 < \frac{-1}{\lambda} < -\frac{1}{1 + \sqrt{2}} = -\left(\frac{1}{1 + \sqrt{2}} \cdot \frac{1 - \sqrt{2}}{1 - \sqrt{2}}\right) = -(\sqrt{2} - 1).$$

Assim,

$$-1 < \lambda' < 1 - \sqrt{2}. \quad (3.4)$$

Dessa forma, somando as Equações (3.1) e (3.4), segue que

$$1 + (-1) < \lambda + \lambda' < 1 + \sqrt{2} + (1 - \sqrt{2}) \Rightarrow 0 < \lambda + \lambda' < 2 \Rightarrow 0 < \frac{\lambda + \lambda'}{2} < 1,$$

o que é uma absurdo uma vez que $\frac{\lambda + \lambda'}{2} \in \mathbb{Z}$. Portanto, $\lambda\lambda' \neq -1$.

Isso completa a prova de que não existem unidades de $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ entre 1 e $1 + \sqrt{2}$. Agora, seja $\eta > 1$ uma unidade qualquer. Como não existem unidades entre 1 e $1 + \sqrt{2}$, segue que devemos ter

$$\eta \geq 1 + \sqrt{2}.$$

Assim, existe um único inteiro positivo n tal que

$$(1 + \sqrt{2})^n \leq \eta < (1 + \sqrt{2})^{n+1}.$$

Deste modo,

$$\frac{(1 + \sqrt{2})^n}{(1 + \sqrt{2})^n} \leq \frac{\eta}{(1 + \sqrt{2})^n} < \frac{(1 + \sqrt{2})^{n+1}}{(1 + \sqrt{2})^n} \Rightarrow 1 < \eta(1 + \sqrt{2})^{-n} < (1 + \sqrt{2}).$$

Como $\eta(1 + \sqrt{2})^{-n}$ é uma unidade de $\mathbb{Z} + \mathbb{Z}\sqrt{2}$, segue que

$$\eta = (1 + \sqrt{2})^n, \quad \text{onde } n \in \mathbb{N}. \quad (3.5)$$

Observe que se tomarmos η uma unidade com $-1 < \eta < 0$, segue que

$$-1 < \eta < 0 \Rightarrow -1 > \frac{1}{\eta} > 0 \Rightarrow -\frac{1}{\eta} > 1,$$

ou seja, $-\frac{1}{\eta}$ seria uma unidade com $-\frac{1}{\eta} > 1$. Assim, pela Equação (3.5), segue que existe $n \in \mathbb{N}$ tal que $-\frac{1}{\eta} = (1 + \sqrt{2})^n$. Assim,

$$-\frac{1}{\eta} = (1 + \sqrt{2})^n \Rightarrow \frac{-1}{(1 + \sqrt{2})^n} = \eta \Rightarrow \eta = -(1 + \sqrt{2})^{-n}, \quad \text{onde } n \in \mathbb{N}.$$

Por outro lado, se η é uma unidade com $\eta < -1$, então $-\eta > 1$. Consequentemente, pela Equação (3.5), segue que existe $n \in \mathbb{N}$ tal que

$$-\eta = (1 + \sqrt{2})^n.$$

Logo,

$$\eta = -1(1 + \sqrt{2})^n, \quad \text{com } n \in \mathbb{N},$$

e assim, $\pm 1 = \pm(1 + \sqrt{2})^0$. Portanto, toda unidade η é dada por

$$\eta = \pm(1 + \sqrt{2})^k, \quad \text{onde } k \in \mathbb{Z},$$

ou seja, se $\eta \in U(\mathbb{Z} + \mathbb{Z}\sqrt{2})$, então $\eta \in \mathbb{Z} + \mathbb{Z}\sqrt{2}$, e portanto,

$$U(\mathbb{Z} + \mathbb{Z}\sqrt{2}) \simeq \mathbb{Z}_2 \times \mathbb{Z},$$

provando o teorema. □

3.3 A equação $x^2 - my^2 = 1$

A equação $x^2 - my^2 = 1$ com $x, y \in \mathbb{Z}$ é conhecida como a equação de Pell, pois Euler atribuiu ao matemático inglês John Pell um método para solucionar essas equações. Entretanto, este método foi encontrado por outro matemático inglês, William Brouncker, em uma série de cartas para Pierre de Fermat. Apesar disso, Lagrange foi o primeiro matemático a provar que a equação $x^2 - my^2 = 1$ tem infinitas soluções em inteiros x e y .

Nosso objetivo, nesta seção, é mostrar que existem inteiros x e y com $(x, y) \neq (\pm 1, 0)$ tal que $x^2 - my^2 = 1$, onde m é um inteiro positivo que não é quadrado perfeito, onde esse resultado afirma que $x + y\sqrt{m} (\neq \pm 1) \in U(\mathcal{O}_{\mathbb{K}})$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{m})$.

Teorema 3.3.1. *Se m é um inteiro positivo que não é um quadrado perfeito (em outras palavras, é livre de quadrados), então existem inteiros x e y com $(x, y) \neq (\pm 1, 0)$ tais que*

$$x^2 - my^2 = 1.$$

Demonstração. Seja N um inteiro positivo não nulo. Mostremos, primeiramente, que existem inteiros x e y tais que

$$0 < |x - y\sqrt{m}| < \frac{1}{N}, \quad \text{onde } 0 < y \leq N. \quad (3.6)$$

Para isso, dividimos o intervalo $0 < x \leq 1$ em N subintervalos satisfazendo

$$\frac{2}{N} < x \leq \frac{r+1}{N}, \quad \text{onde } r = 0, 1, \dots, N-1. \quad (3.7)$$

Note que cada subintervalo tem comprimento $\frac{1}{N}$. Para $i = 0, 1, \dots, N$, sejam os inteiros x_i e y_i definidos como

$$\begin{cases} x_i = [i\sqrt{m}] + 1 \\ y_i = i, \end{cases}$$

onde $[k]$, com $k \in \mathbb{R}$, denota a parte inteira do número real k . Assim, para $i = 0, \dots, N_i$, segue que

$$\begin{aligned} [i\sqrt{m}] &\leq i\sqrt{m} < [i\sqrt{m}] + 1 \Rightarrow x_i - 1 \leq y_i\sqrt{m} < x_i \\ &\stackrel{+x_i}{\Rightarrow} -x_i + x_i - 1 \leq -x_i + y_i\sqrt{m} < -x_i + x_i \Rightarrow -x_i + x_i \\ &\Rightarrow -1 \leq -x_i + y_i\sqrt{m} < 0 \stackrel{(-1)}{\Rightarrow} 0 < x_i - y_i\sqrt{m} \leq 1. \end{aligned}$$

Portanto, existem $(N+1)$ números dados por $(x_i - y_i\sqrt{m})$ em $(0, 1]$. Mas, observe que ao menos dois desses números estão no mesmo subintervalo $\left(\frac{r}{N}, \frac{r+1}{N}\right)$, uma vez que existem N subintervalos e $N+1$ números. Dessa forma, existem inteiros i e j com $i \neq j$, $0 \leq i \leq N$ e $0 \leq j \leq N$, tal que

$$\frac{r}{N} < x_i - y_i\sqrt{m} \leq \frac{r+1}{N} \quad (3.8)$$

e

$$\frac{r}{N} < x_j - y_j\sqrt{m} \leq \frac{r+1}{N}. \quad (3.9)$$

Como $(x_i - y_i\sqrt{m})$ e $(x_j - y_j\sqrt{m})$ estão num mesmo intervalo $\left(\frac{r}{N}, \frac{r+1}{N}\right)$, podemos supor, sem perda de generalidade,

$$x_i - y_i\sqrt{m} \geq x_j - y_j\sqrt{m} \Rightarrow (x_i - y_i\sqrt{m}) - (x_j - y_j\sqrt{m}) \geq 0.$$

Dessa forma, como cada intervalo tem tamanho $\frac{1}{N}$, segue que

$$0 \leq (x_i - y_i\sqrt{m}) - (x_j - y_j\sqrt{m}) < \frac{1}{N}.$$

Note, ainda que, $y_i - y_j = i - j \neq 0$. Assim, defina os inteiros x e y da seguinte forma

$$(x, y) = \begin{cases} (x_i - x_j, y_i - y_j), & \text{se } y_i - y_j > 0; \\ (x_j - x_i, y_j - y_i), & \text{se } y_i - y_j < 0. \end{cases}$$

Assim, $0 \leq |x - y\sqrt{m}| < \frac{1}{N}$, implica que $-\frac{1}{N} < x - y\sqrt{m} < \frac{1}{N}$, com $y > 0$, e $y = |y| = |y_i - y_j| = |i - j| \leq N$. Isso completa a prova da desigualdade (3.6). Agora, mostremos que existem infinitos pares de inteiros (x, y) , com $y \neq 0$, tal que

$$0 < |x^2 - my^2| < 1 + 2\sqrt{m}. \quad (3.10)$$

Seja N_1 um inteiro positivo. Pela Equação (3.6), segue que existem inteiros x_1 e y_1 tais que

$$0 < |x_1 - y_1\sqrt{m}| < \frac{1}{N_1}, \quad \text{onde } 0 < y_1 \leq N_1.$$

Agora, seja N_2 um inteiro positivo tal que

$$N_2 > \frac{1}{|x_1 - y_1\sqrt{m}|}.$$

Dessa forma, pela Equação (3.6), segue que existem inteiros x_2 e y_2 tais que

$$0 < |x_2 - y_2\sqrt{m}| < \frac{1}{N_2}, \quad \text{com } 0 < y_2 \leq N_2.$$

Prosseguindo dessa forma, após obter N_r, x_r e y_r , com $r = 1, 2, \dots, k-1$, escolhamos N_k satisfazendo

$$N_k > \frac{1}{|x_{k-1} - y_{k-1}\sqrt{m}|}$$

e inteiros x_k e y_k positivos tais que

$$0 < |x_k - y_k\sqrt{m}| < \frac{1}{N_k}, \quad \text{onde } 0 < y_k \leq N_k.$$

Desse modo,

$$\begin{aligned} 0 &< |x_k - y_k\sqrt{m}| < \frac{1}{N_k} < |x_{k-1} - y_{k-1}\sqrt{m}| < \frac{1}{N_{k-1}} \\ &< \dots < |x_2 - y_2\sqrt{m}| < \frac{1}{N_2} < |x_1 - y_1\sqrt{m}| < \frac{1}{N_1}. \end{aligned}$$

Dessa forma, (x_k, y_k) , onde $k \in \mathbb{N}^*$, é um sequência infinita de pares de inteiros satisfazendo

$$0 < |x_k - y_k\sqrt{m}| < \frac{1}{N_k} \leq \frac{1}{y_k}, \quad \text{pois } y_k \leq N_k.$$

Como, por hipótese m é livre de quadrados e $y_k > 0$, para todo k , segue que

$$\begin{aligned} 0 < |x_k + y_k\sqrt{m}| &= |x_k + y_k\sqrt{m} + y_k\sqrt{m} - y_k\sqrt{m}| = |x_k - y_k\sqrt{m} + \underbrace{2y_k\sqrt{m}}_{>0}| \leq |x_k - \\ &\underbrace{y_k\sqrt{m} + 2y_k\sqrt{m}}_{\geq 0}| = |x_k - y_k\sqrt{m}| + 2y_k\sqrt{m} < \frac{1}{y_k} + 2y_k\sqrt{m} \Rightarrow |x_k + y_k\sqrt{m}| < \frac{1}{y_k} + 2y_k\sqrt{m}. \end{aligned}$$

Como

$$|x^2 - my^2| = |(x_k - \sqrt{m}y_k)(x_k + \sqrt{m}y_k)| = \underbrace{|x_k - \sqrt{m}y_k|}_{< \frac{1}{y_k}} \underbrace{|x_k + \sqrt{m}y_k|}_{< \frac{1}{y_k}} + 2y_k\sqrt{m},$$

para $k = 1, 2, \dots$, segue que

$$0 < |x_k^2 - my_k^2| < \frac{1}{y_k} \left(\frac{1}{y_k} + 2y_k\sqrt{m} \right) = \frac{1}{y_k^2} + 2\sqrt{m} \leq 1 + 2\sqrt{m}.$$

Mas, como $x^2 - my^2 \in \mathbb{Z}$, segue que

$$x^2 - my^2 = t \tag{3.11}$$

com $t \in \mathbb{Z}$, e pela Equação (3.10), segue que

$$0 < |t| < 1 + 2\sqrt{m}.$$

Observe, ainda, que existem infinitas soluções distintas de inteiros (x, y) para a Equação (3.11), uma vez que $(x, y) = (x_k, y_k)$, onde $k \in \mathbb{N}^*$. Substituindo x por $-x$ e y por $-y$ se necessário, segue que a Equação (3.11) tem infinitas soluções de inteiros positivos x e y . Agora, seja t tal que a Equação (3.11) tenha infinitas soluções em inteiros positivos x, y , com $|t|$ minimal. Como m não é um quadrado perfeito, segue que $|t| > 0$. Mostremos que $\text{mdc}(t, y) = 1$ para uma quantidade infinita de soluções (na verdade, para todos exceto por uma quantidade finita). Suponha que $(t, y) > 1$. Como $t \in \mathbb{Z}$, t possui apenas uma quantidade finita de fatores primos. Assim, existe ao menos um primo p divisor de t , onde cada Equação (3.11) possui uma quantidade infinita de soluções em x e y com $p|y$. Para cada uma dessas soluções, segue que $p|x$, então $p^2|t$. Dessa forma,

$$x^2 - my^2 = \frac{1}{p^2}$$

possui infinitas soluções em inteiros positivos x e y , contradizendo que $|t|$ é o menor inteiro com essa propriedade. Seja (x, y) uma das soluções de (3.11) em inteiros positivos tal que $(t, y) = 1$. Seja u o inteiro tal que

$$\underbrace{uy \equiv 1 \pmod{t}}_{t|uy-1}, \quad 0 < u < |t|.$$

Como existem $|t|$ classes de equivalência módulo t , pela Teoria Elementar dos Números, segue que podemos encontrar duas soluções, digamos (x_1, y_1) e (x_2, y_2) , tais que

$$u_1x_1 \equiv u_2x_2 \pmod{t}.$$

Com isso,

$$\begin{aligned} \frac{x_1 + \sqrt{m}y_1}{x_2 + \sqrt{m}y_2} &= \frac{x_1 + \sqrt{m}y_1}{x_2 + \sqrt{m}y_2} \cdot \frac{x_2 - \sqrt{m}y_2}{x_2 - \sqrt{m}y_2} = \frac{(x_1 + \sqrt{m}y_1)(x_2 - \sqrt{m}y_2)}{x_2^2 - \sqrt{m}y_2^2} \\ &= \frac{x_1x_2 - \sqrt{m}x_1y_2 + \sqrt{m}x_2y_1 - my_1y_2}{t} \\ &= \frac{(x_1x_2 - my_1y_2) + \sqrt{m}(x_2y_1 - x_1y_2)}{t}. \end{aligned}$$

Logo,

$$\frac{x_1 + \sqrt{m}y_1}{x_2 + \sqrt{m}y_2} = x + \sqrt{m}y, \quad (3.12)$$

onde $x = \frac{(x_1x_2 - my_1y_2)}{t}$, $y = \frac{(x_2y_1 - x_1y_2)}{t}$. Como (x_1, y_1) , (x_2, y_2) são pares de inteiros positivos e t é inteiro, então x e y são racionais. Queremos mostrar que $x \in \mathbb{Z}$ e $y \in \mathbb{Z}$. Para isso, observe que

$$\begin{aligned} u_1u_2(x_2y_1 - y_2x_1) &= (u_1u_2)(x_2y_1) - (u_1u_2)(y_2x_1) \\ &= (u_1y_1)(u_2x_2) - (u_2y_2)(u_1x_1) \equiv u_2x_2 - u_1x_1 \equiv 0 \pmod{t}. \end{aligned}$$

Note que $(u_1u_2, t) = 1$. Assim,

$$(u_1u_2)(x_2y_1 - y_2x_1) \equiv 0 \pmod{t} \Rightarrow x_2y_1 - y_2x_1 \equiv 0 \pmod{t} \Rightarrow y \in \mathbb{Z}.$$

Por outro lado,

$$(u_1u_2)(x_1x_2 - my_1y_2) = (u_1u_2)(x_1x_2) - m(u_1u_2)(y_1y_2) = (u_1x_1)(u_2x_2) - m(u_1y_1)(u_2y_2).$$

Como

$$\begin{cases} u_1x_1 \equiv u_2x_2 \pmod{t} \\ u_1y_1 \equiv u_2y_2 \pmod{t}, \end{cases}$$

segue que

$$(u_1x_1)(u_2x_2) - m(u_1y_1)(u_2y_2) \equiv (u_1x_1)^2 - m(u_1y_1)^2.$$

Agora, note que

$$(u_1x_1)^2 - m(u_1y_1)^2 = u_1^2x_1^2 - mu_1^2y_1^2 = u_1^2(x_1^2 - my_1^2) = u_1^2t \equiv 0 \pmod{t}.$$

Juntando todas essas informações, podemos concluir que

$$(u_1u_2)(x_1x_2 - my_1y_2) \equiv 0 \pmod{t}.$$

Como $(u_1u_2, t) = 1$, segue que $x_1x_2 - my_1y_2 \equiv 0 \pmod{t}$. Deste modo, $x = \frac{x_1x_2 - my_1y_2}{t} \in \mathbb{Z}$. Voltando a Equação (3.12), segue que

$$\frac{x_1 + \sqrt{m}y_1}{x_2 + \sqrt{m}y_2} = x + \sqrt{m}y \Rightarrow x_1 + \sqrt{m}y_1 = (x + \sqrt{m}y)(x_2 + \sqrt{m}y_2).$$

Logo,

$$t = x_1^2 - my_1^2 = (x_2^2 - \sqrt{m}y_2^2)(x^2 - \sqrt{m}y^2) = t(x^2 - my^2) \Rightarrow (x^2 - my^2) = \frac{t}{t} = 1.$$

Agora, seja $(x, y) = (\pm 1, 0)$. Pela Equação (3.12), segue que

$$x_1 + \sqrt{m}y_1 = \pm(x_2 + \sqrt{m}y_2) \Rightarrow (x_1, y_1) = \pm(x_2, y_2).$$

Mas, como $(x_1, y_1), (x_2, y_2)$ são pares de inteiros positivos, segue que

$$(x_1, y_1) = (x_2, y_2).$$

Mas, isso não ocorre, uma vez que definimos esses pares como soluções distintas da Equação (3.11). Portanto, mostramos a existência de um par de inteiros $(x, y) \neq (\pm 1, 0)$ tal que $x^2 - my^2 = 1$, como queríamos. $\square$

3.4 Unidades de norma 1

Seja m um inteiro positivo livre de quadrados. Pelo Teorema 3.2.1, segue que existem inteiros positivos x e y tais que $x^2 - my^2 = 1$. Consequentemente, $\lambda = x + y\sqrt{m}$ é uma unidade de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{Q}(\sqrt{m}) = \mathbb{K}$, tal que $\lambda > 1$ e $N(\lambda) = 1$, uma vez que $x^2 - my^2 = 1 \Leftrightarrow (x - \sqrt{m}y) \underbrace{(x + \sqrt{m}y)}_{>0} = 1$.

Como $\lambda^n \rightarrow \infty$, quando $n \rightarrow \infty$, segue que $\mathcal{O}_{\mathbb{K}}$ possui infinitas unidades de norma 1, que são dadas pelas potências de λ , ou seja, $\{\lambda^n | n \in \mathbb{Z}\}$. Todas essas unidades são da forma $u + v\sqrt{m}$, onde u e v são inteiros da forma $u^2 - mv^2 = 1$. Entretanto, quando $m \equiv 1 \pmod{4}$, existem unidades em $\mathcal{O}_{\mathbb{K}}$ da forma $\frac{(u + v\sqrt{m})}{2}$, onde u e v são inteiros ímpares.

Exemplo 3.4.1. O número $\frac{3 + \sqrt{5}}{2}$ é uma unidade de norma 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$, uma vez que

$$\left(\frac{3 + \sqrt{5}}{2}\right) \left(\frac{3 - \sqrt{5}}{2}\right) = \frac{3^2 - \sqrt{5}^2}{4} = \frac{9 - 5}{4} = \frac{4}{4} = 1, \text{ onde } \frac{3 + \sqrt{5}}{2} > 1.$$

Por outro lado, $\mathcal{O}_{\mathbb{Q}(\sqrt{17})}$ não contém unidades da forma $\frac{u + v\sqrt{17}}{2}$ quando u e v são inteiros ímpares, uma vez que se existe alguma unidade dessa forma, então

$$\left(\frac{u + v\sqrt{17}}{2}\right) \cdot \left(\frac{u - v\sqrt{17}}{2}\right) = 1 \Leftrightarrow u^2 - 17v^2 = 4.$$

Note que $\pm 4 \equiv 4 \pmod{8}$, entretanto $u^2 - 17v^2 \not\equiv 4 \pmod{8}$, quando u e v são inteiros ímpares, o que é um absurdo. Assim, $\mathcal{O}_{\mathbb{Q}(\sqrt{17})}$ não possuem unidades com essas propriedades.

Agora, considere $\lambda = x + y\sqrt{m}$ uma unidade de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, de norma 1, com x e y inteiros e, na possibilidade do caso $m \equiv 1 \pmod{4}$, de $\frac{x}{2}$ e $\frac{y}{2}$ serem inteiros ímpares. Mostramos, a seguir, como os sinais de x e y determinam a qual dos quatro intervalos $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ ou $(1, +\infty)$, o número λ pertence.

Teorema 3.4.2. *Seja m um inteiro positivo livre de quadrados. Se x e y são inteiros ou $\frac{x}{2}$ e $\frac{y}{2}$ são inteiros ímpares tais que $x^2 - my^2 = 1$, então*

1. $x + y\sqrt{m} > 1 \Leftrightarrow x > 0$ e $y > 0$;
2. $0 < x + y\sqrt{m} < 1 \Leftrightarrow x > 0$ e $y < 0$;
3. $-1 < x + y\sqrt{m} < 0 \Leftrightarrow x < 0$ e $y > 0$;
4. $x + y\sqrt{m} < -1 \Leftrightarrow x < 0$ e $y < 0$.

Demonstração. A prova será dividida em quatro partes, uma para cada intervalo.

1. Por definição, segue que $x^2 - my^2 = 1 = (x + \sqrt{m}y)(x - \sqrt{m}y) = 1$. Como $x + \sqrt{m}y > 1$, segue que $0 < (x - \sqrt{m}y) < 1$. Note ainda que podemos escrever x e y das seguintes formas, sem perda de generalidade:

$$\left\{ \begin{array}{l} x = \frac{2}{2}x = \frac{x}{2} + \frac{x}{2} + \left(\frac{y\sqrt{m}}{2} - \frac{y\sqrt{m}}{2} \right) = \frac{1}{2} \left(\underbrace{(x + y\sqrt{m})}_{>1} + \underbrace{(x - y\sqrt{m})}_{>0} \right) > \frac{1}{2} > 0 \\ y = y \cdot \frac{2\sqrt{m}}{2\sqrt{m}} = \frac{1}{2\sqrt{m}} (2y\sqrt{m} + -x + x) = \frac{1}{2\sqrt{m}} \cdot \left(\underbrace{(x + y\sqrt{m})}_{>1} - \underbrace{(x - y\sqrt{m})}_{\in(0,1)} \right) \\ > \frac{1-1}{2\sqrt{m}} > 0. \end{array} \right.$$

Portanto, $x > 0$ e $y > 0$, como queríamos. Reciprocamente, se $x > 0$ e $y > 0$, com $x, y \in \mathbb{Z}_+$, então

$$x \geq \frac{1}{2}, y \geq \frac{1}{2} \Rightarrow x + y\sqrt{m} \geq \frac{1}{2} + \frac{1}{2}\sqrt{m} = \frac{1 + \sqrt{m}}{2} \geq \frac{1 + \sqrt{2}}{2} > 1,$$

uma vez que $m \in \mathbb{Z}$ é livre de quadrados, ou seja, $\sqrt{m} > \sqrt{2}$.

2. Se $0 < x + y\sqrt{m} < 1$, então $x - y\sqrt{m} > 1$. Reescrevendo x e y de modo análogo ao item 1, segue que

$$\left\{ \begin{array}{l} x = \frac{1}{2} ((x + y\sqrt{m}) + (x - y\sqrt{m})) > \frac{1}{2} > 0 \\ y = \frac{1}{2\sqrt{m}} ((x + y\sqrt{m}) - (x - y\sqrt{m})) < \frac{1-1}{2\sqrt{m}} - 0 \end{array} \right. \Rightarrow x > 0, y < 0.$$

Reciprocamente,

$$\left\{ \begin{array}{l} x > 0 \\ y < 0 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x > 0 \\ -y > 0 \end{array} \right. \Rightarrow \left\{ \begin{array}{l} x \geq \frac{1}{2} \\ -y \geq \frac{1}{2} \end{array} \right. .$$

Dessa forma,

$$x - y\sqrt{m} \geq \frac{1}{2} + \frac{1}{2}\sqrt{m} \geq \frac{1 + \sqrt{m}}{2} \geq \frac{1 + \sqrt{2}}{2} > 1 \Rightarrow x - y\sqrt{m} > 1.$$

Como $\underbrace{(x - y\sqrt{m})}_{\geq 1} (x + y\sqrt{m}) = 1$, segue que $0 < x + y\sqrt{m} < 1$.

3. Se $-1 < x + y\sqrt{m} < 0$, então $(x - y\sqrt{m}) > -1$. Assim,

$$\left\{ \begin{array}{l} x = \frac{1}{2} \left(\overbrace{(x + y\sqrt{m}) + (x - y\sqrt{m})}^{<0} \right) < \frac{-1}{2} < 0 \\ y = \frac{1}{2\sqrt{m}} \left(\underbrace{(x + y\sqrt{m})}_{>0} - \underbrace{(x - y\sqrt{m})}_{>0} \right) > 0. \end{array} \right.$$

Logo, $x < 0$ e $y > 0$.

$$\text{Reciprocamente, se } \begin{cases} x < 0 \\ y > 0 \end{cases} \Rightarrow \begin{cases} -x > 0 \\ y > 0 \end{cases} \Rightarrow \begin{cases} -x \geq \frac{1}{2} \\ y \geq \frac{1}{2} \end{cases}.$$

Assim,

$$\begin{aligned} -x + y\sqrt{m} &\geq \frac{1}{2} + \frac{1}{2}\sqrt{m} \Rightarrow -(x - y\sqrt{m}) \geq \frac{1 + \sqrt{m}}{2} \geq \frac{1 + \sqrt{2}}{2} > 1 \\ \Rightarrow -(x - y\sqrt{m}) > 1 &\Rightarrow (x - y\sqrt{m}) < -1. \end{aligned}$$

Mas, como $\underbrace{(x - y\sqrt{m})}_{\leq -1}(x + y\sqrt{m}) = 1$, segue que $(x + y\sqrt{m}) < 0$. Mais ainda, como

o produto deve ser igual a 1, segue que $0 > x + y\sqrt{m} < 0$.

4. Se $x + y\sqrt{m} < -1$, de modo análogo ao item 1, multiplicando a desigualdade por -1 , segue que $x < 0$ e $y < 0$. Reciprocamente, sejam $x < 0$ e $y < 0$. Pelo item 1, segue que $(x' + y'\sqrt{m}) > 1$, onde $x' > 0$ e $y' > 0$. Assim, sejam $x' = -x$ e $y' = -y$. Daí,

$$-x - y\sqrt{m} > 1 \Leftrightarrow -(x + y\sqrt{m}) > 1 \Leftrightarrow x + y\sqrt{m} < -1,$$

o que prova o teorema. $\square$

Definição 3.4.3. (Unidade fundamental de norma 1) Tome m um inteiro positivo livre de quadrados. Seja

$$S_m = \{(x, y) \mid x \in \mathbb{N}, y \in \mathbb{N}\}, \text{ se } m \equiv 2, 3 \pmod{4}, \text{ ou}$$

$$S_m = \left\{ \left(\frac{x}{2}, \frac{y}{2} \right) \mid x \in \mathbb{N}, y \in \mathbb{N}, x \equiv y \pmod{2} \right\}, \text{ se } m \equiv 1 \pmod{4}.$$

Considere $(a, b) \in S_m$ a solução de $a^2 - mb^2 = 1$ no qual a é o menor entre eles. Seja $\epsilon = a + b\sqrt{m}$ tal que ϵ é a unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1. A unidade ϵ é chamada **unidade fundamental de norma 1 de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$** .

Observação 3.4.4. Como na Definição 3.4.3, obtemos os seguintes fatos.

1. A existência do par (a, b) é garantida pelo Teorema 3.2.1.
2. Para $\epsilon = a + b\sqrt{m}$, com $a, b \in \mathbb{N}$, segue que

$$\begin{cases} \epsilon \geq 1 + \sqrt{m} \geq 1 + \sqrt{2}, & \text{se } m \equiv 2, 3 \pmod{4}. \\ \epsilon \geq \frac{1 + \sqrt{m}}{2} \geq \frac{1 + \sqrt{5}}{2}, & \text{se } m \equiv 1 \pmod{4}. \end{cases}$$

Dessa forma, segue que em ambos casos $\epsilon > 1$. Em outras palavras, a unidade fundamental de norma 1 de $\mathcal{O}_{\mathbb{K}}$, $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, é sempre maior do que 1.

Uma dúvida natural é como as unidades quaisquer de norma 1 de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ se relacionam com a unidade fundamental de norma 1. Pretendemos responder essa questão com os próximos Teoremas.

A seguir, considere sempre m um inteiro livre de quadrados.

Teorema 3.4.5. Se ϵ é a unidade fundamental de norma 1 de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, então ϵ é a menor unidade em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1 maior do que 1.

Demonstração. Pela Definição (3.4.3), segue que

$$\epsilon = a + b\sqrt{m} = \begin{cases} (a, b) \in S_m, \\ a^2 - mb^2 = 1, \\ a \text{ é mínimo.} \end{cases}$$

uma vez que ϵ é a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$. Suponha que exista $\epsilon_1 \in U(\mathcal{O}_{\mathbb{Q}(\sqrt{m})})$ de norma 1 tal que

$$1 < \epsilon_1 < \epsilon.$$

Pelos Teoremas 2.4.8 e pelo Teorema 3.4.2, segue que

$$\epsilon_1 = a_1 + b_1\sqrt{m}, \begin{cases} (a_1, b_1) \in S_m \\ a_1^2 - mb_1^2 = 1. \end{cases}$$

Pela minimalidade de a , segue que $a_1 > a$. Dessa forma

$$a_1^2 - mb_1^2 = 1 \Rightarrow b_1^2 = \frac{1 - a_1^2}{(-m)} = \frac{a_1^2 - 1}{m} > \frac{a^2 - 1}{m} = b^2 \Rightarrow b_1^2 > b^2 \Rightarrow b_1 > b.$$

Assim,

$$\epsilon_1 = a_1 + b_1\sqrt{m} > a + b\sqrt{m} = \epsilon \Rightarrow \epsilon_1 > \epsilon.$$

Entretanto isso contradiz a hipótese de que $\epsilon_1 < \epsilon$. Portanto, não existe uma unidade ϵ_1 menor do que ϵ , provando que a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é a menor unidade de norma 1 maior do que 1. $\square$

Teorema 3.4.6. *Se ϵ é a unidade fundamental de norma 1 de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, então toda unidade em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1 é da forma $\pm\epsilon^n$, para algum inteiro n .*

Demonstração. Seja η uma unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1. Seja η^* uma unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1 tal que

$$\eta^* = \begin{cases} \eta, & \text{se } \eta \geq 1; \\ \frac{1}{\eta}, & \text{se } 0 < \eta < 1; \\ -\frac{1}{\eta}, & \text{se } -1 < \eta < 0; \\ -\eta, & \text{se } \eta \leq -1. \end{cases} \quad (3.13)$$

Pela Equação (3.13), segue que $\eta^* \geq 1$. Seja k o único inteiro não negativo tal que

$$\epsilon^k \leq \eta^* < \epsilon^{k+1}.$$

Como o produto de unidades é uma unidade, segue que $\eta^*\epsilon^{-k}$ é uma unidade de norma 1 que satisfaz

$$1 \leq \eta^*\epsilon^{-k} < \epsilon.$$

Pelo Teorema 3.4.5, segue que não existe ϵ_1 unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1 estritamente entre 1 e ϵ . Logo,

$$\eta^*\epsilon^{-k} = 1 \Rightarrow \eta^* = \epsilon^k.$$

Assim, pela Equação (3.13), segue que

$$\epsilon^k = \eta^* = \begin{cases} \eta, & \text{se } \eta \in [-1, \infty); \\ \frac{1}{\eta}, & \text{se } \eta \in (0, 1); \\ -\frac{1}{\eta}, & \text{se } \eta \in (-1, 0); \\ -\eta, & \text{se } \eta \in (-\infty, 1]. \end{cases}$$

Assim, $\eta = \pm\epsilon^n$, para alguma escolha de sinal e algum inteiro n . $\square$

Teorema 3.4.7. *Seja ϵ a unidade fundamental de norma 1 de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$. Se τ é a unidade de norma 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ tal que $\tau > 1$ e toda unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1 é da forma $\pm\tau^k$ para inteiros k , então $\tau = \epsilon$.*

Demonstração. Por hipótese, segue que τ é uma unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ com norma maior do que 1 tal que $\tau > 1$ e

$$\epsilon = \pm\tau^l, \text{ para algum } l \in \mathbb{Z}.$$

Mas, pelo Teorema 3.4.6, segue que

$$\tau = \pm\epsilon^n, \text{ para algum } n \in \mathbb{Z}.$$

Logo,

$$\epsilon = \pm(\pm\epsilon^n)^l = \pm\epsilon^{ln} \Rightarrow \epsilon^{ln} = \pm\epsilon \Rightarrow \epsilon^{ln-1} = \pm 1 \Rightarrow (\epsilon^{ln-1})^2 = (\pm 1)^2 \Rightarrow \epsilon^{2(ln-1)} = 1.$$

Se $(ln - 1) \neq 0$, então ϵ é uma raiz da unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$. Mas, como $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é um corpo real, segue que as únicas raízes da unidade em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ são ± 1 . Dessa forma, $\epsilon = \pm 1$. Entretanto isso contradiz a hipótese de que $\epsilon > 1$. Portanto,

$$(ln - 1) = 0 \Rightarrow ln = 1 \Rightarrow l = n = \pm 1,$$

ou seja, $\tau = \pm\epsilon$ ou $\tau = \pm\epsilon^{-1}$. Como $\tau > 1$ e $\epsilon > 1$, segue que $\tau = \epsilon$, como queríamos demonstrar. $\square$

3.5 Unidades de norma -1

Seja m um inteiro positivo livre de quadrados. Na Seção 3.3, já observamos que o anel de inteiros do corpo quadrático real $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ sempre contém infinitas unidades de norma 1, entretanto esses corpos podem possuir ou não possuir unidades de norma -1 . Por exemplo, $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$ tem unidade a $(1 + \sqrt{2})$ que tem norma -1 enquanto que $\mathcal{O}_{\mathbb{Q}(\sqrt{3})}$ não contém nenhuma unidade de norma -1 .

A seguir, vamos mostrar que se $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ contém unidades de norma -1 , então existe uma única unidade $\sigma > 1$ em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma -1 tal que todas as outras unidades de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ são dadas por $\pm\sigma^{2k-1}$, para todo $k \in \mathbb{Z}$. Além disso, todas as unidades em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1 podem ser escritas como $\pm\sigma^{2k}$, para todo $k \in \mathbb{Z}$.

Teorema 3.5.1. *Seja m um inteiro livre de quadrados. Se $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ possui unidades de norma -1 , então existe uma única unidade $\sigma > 1$ de norma -1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ tal que toda unidade em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é da forma $\pm\sigma^n$, para algum inteiro n .*

Demonstração. Seja ρ uma unidade em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma -1 . Denote por ρ' seu conjugado. Pela definição de norma, segue que

$$\rho\rho' = N(\rho) = -1.$$

Assim,

$$(\pm\rho')^2 = (-1)^2 \Rightarrow \rho^2(\rho')^2 = 1,$$

ou seja, ρ é uma unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1. Pelo Teorema 3.4.6, segue que $\rho^2 = \pm\epsilon^n$, para algum $n \in \mathbb{Z}$, onde ϵ é a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1. Como $\rho^2 > 0$ e $\epsilon^n > 0$, segue que

$$\rho^2 = \epsilon^n.$$

Se n é par, podemos reescrevê-lo como $n = 2k$, com $k \in \mathbb{Z}$. Assim,

$$\rho^n = \epsilon^{2k} = (\epsilon^k)^2 \Rightarrow \rho = \pm\epsilon^k.$$

Logo,

$$N(\rho) = N(\pm\epsilon^k) = [N(\epsilon)]^k = 1.$$

Mas, isso é um absurdo, uma vez que contradiz a hipótese de que $N(\rho) = -1$. Dessa forma, n deve ser ímpar. Assim, se $n = 2l + 1$, para algum $l \in \mathbb{Z}$, então

$$\rho^2 = \epsilon^{2l+1} = \epsilon^{2l} \cdot \epsilon \Rightarrow \epsilon = \rho^2 \cdot \epsilon^{-(2l)} = \rho^2 \cdot \epsilon^{2(-l)} = \rho^2 \cdot (\epsilon^{-l})^2 \Rightarrow \epsilon = (\rho \cdot \epsilon^{-l})^2.$$

Agora, defina $\sigma = \rho\epsilon^{-l}$ de forma que σ é a unidade de norma -1 tal que

$$\epsilon = \sigma^2.$$

Se μ é a unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma -1 , então $(\mu\rho^{-1})$ é a unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1, e portanto, pelo Teorema 3.4.6, segue que

$$\mu\rho^{-1} = \pm\epsilon^k, \text{ para algum } k \in \mathbb{Z}.$$

Como $\rho = \epsilon^l\sigma$ e $\epsilon = \sigma^2$, segue que

$$\mu = \pm\epsilon^k \cdot \rho = \pm\epsilon^k \cdot \epsilon^l \cdot \sigma = \pm\epsilon^{k+l} \cdot \sigma = \pm(\sigma^2)^{k+l} \cdot \sigma = \pm\sigma^{2(k+l)+1} \Rightarrow \mu = \sigma^{2(k+l)+1}.$$

Contudo, se μ é uma unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma 1, então pelo Teorema 3.4.6, segue que

$$\mu = \pm\epsilon^k, \text{ para algum } k \in \mathbb{Z}.$$

Como $\epsilon = \sigma^2$, segue que $\mu = \pm\epsilon^k = \pm\sigma^{2k}$. Portanto, toda unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é da forma

$$\pm\sigma^n, \text{ onde } n \in \mathbb{Z}.$$

Por fim, note que se n é par, então existem unidades de norma 1 e quando n é ímpar, as unidades de norma -1 . Como queremos $\sigma > 1$, quando necessário, façamos a seguinte substituição:

$$\begin{cases} \frac{1}{\sigma}, & \text{se } 0 < \sigma < 1; \\ -\frac{1}{\sigma}, & \text{se } -1 < \sigma < 0; \\ -\sigma, & \text{se } \sigma < -1. \end{cases}$$

Agora, mostremos que σ é unicamente determinado. Para isso, suponha que σ e τ são duas unidades maiores do que 1 de norma -1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ tais que toda unidade é da forma $\pm\sigma^n$, com $n \in \mathbb{Z}$, e da forma $\pm\tau^q$, com $q \in \mathbb{Z}$. Assim, existem inteiros k e l tais que

$$\sigma = \pm\tau^k \text{ e } \tau = \pm\sigma^l,$$

ou seja,

$$\sigma = \pm(\sigma^l)^k = \pm\sigma^{lk} \Rightarrow \sigma^2 = (\pm\sigma^{lk})^2 = \sigma^{2lk} \Rightarrow \sigma^{2lk} \cdot \sigma^{-2} = 1 \Rightarrow \sigma^{2(kl-1)} = 1.$$

Se $(kl - 1) \neq 0$, então σ é uma raiz da unidade. Mas, como $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é um corpo real, segue que as únicas raízes da unidade são ± 1 . Logo, $\sigma = \pm 1$, o que é uma contradição pois $\sigma > 1$. Dessa forma, $(kl - 1) = 0$ e $k = l = \pm 1$. Assim,

$$\sigma = \pm\tau \text{ ou } \sigma = \pm\tau^{-1}.$$

Como σ e τ são positivos, segue que

$$\sigma = \tau.$$

Portanto, σ é unicamente determinado. □

Definição 3.5.2. (Unidade fundamental de norma -1) Seja m um inteiro positivo livre de quadrados tal que $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ contém unidades de norma -1 . A única unidade $\sigma > 1$ de norma -1 tal que todas as unidades de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ são da forma $\pm\sigma^n$ com $n \in \mathbb{Z}$, é chamada **unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ de norma -1** .

A seguir, mostramos a relação da unidade fundamental ϵ de norma 1 e a unidade fundamental σ de norma -1 , no caso de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ possuir unidades de norma -1 .

Teorema 3.5.3. *Se m é um inteiro positivo livre de quadrados tal que $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ contém unidades de norma -1 , então a unidade fundamental ϵ de norma 1 e a unidade fundamental σ de norma -1 estão relacionadas por*

$$\epsilon = \sigma^2.$$

Demonstração. Pelo Teorema 3.5.1, segue que $\epsilon = \pm\sigma^k$, para algum $k \in \mathbb{Z}$. Como $\sigma > 1$ e $\epsilon > 1$, segue que

$$\epsilon = \sigma^k, \text{ para algum } k \in \mathbb{Z}.$$

Assim,

$$1 = N(\epsilon) = N(\sigma^k) = (N(\sigma))^k = (-1)^k \Rightarrow 1 = (-1)^k \Rightarrow k \text{ é par}.$$

Como k deve ser par, segue que $k = 2g$, com $g \in \mathbb{Z}$. Logo,

$$\epsilon = \sigma^{2g}. \tag{3.14}$$

Note que

$$N(\sigma^2) = (N(\sigma))^2 = (-1)^2 = 1.$$

Dessa forma, σ^2 é uma unidade de norma 1, e portanto, pelo Teorema 3.4.6, segue que

$$\sigma^2 = \pm\epsilon^l, \text{ para algum } l \in \mathbb{Z}.$$

Novamente, como $\sigma > 1$ e $\epsilon > 0$, podemos descartar a possibilidade do sinal ser negativo. Assim,

$$\sigma^2 = \epsilon^l, \text{ para algum } l \in \mathbb{Z}. \tag{3.15}$$

Juntando as Equações (3.14) e (3.15), segue que

$$\epsilon = \sigma^{2g} = (\sigma^2)^g = (\epsilon^l)^g \Rightarrow \epsilon = \epsilon^{lg} \Rightarrow \epsilon^{gl-1} = 1.$$

Como ϵ não é uma raiz da unidade, deduzimos que $(gl - 1) = 0$. Portanto,

$$\epsilon = \sigma^2 \text{ ou } \epsilon = \sigma^{-2}.$$

Mais uma vez, do fato de que $\epsilon > 1$ e $\sigma > 1$, concluimos que

$$\epsilon = \sigma^2,$$

como queríamos. □

3.6 Unidade fundamental

Os Teoremas 3.4.6 e 3.5.3 mostram que todas as unidades de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ são dadas por $\pm\epsilon^n$, com $n \in \mathbb{Z}$, ou por $\pm\sigma^n$, com $n \in \mathbb{Z}$, dependendo se $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ tem apenas unidades de norma 1 ou não. Isso permite definir a unidade fundamental do anel de inteiros $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

Definição 3.6.1. (Unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$) Seja m um inteiro positivo livre de quadrados. A **unidade fundamental** η de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é definida por σ se $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ contém unidades de norma -1 e por ϵ , caso contrário. Note que sempre $\eta > 1$.

Assim, juntando as informações dos Teoremas 3.4.6 e 3.5.3, podemos formular o seguinte resultado.

Teorema 3.6.2. *Se m é um inteiro positivo livre de quadrados, então toda unidade é da forma $\pm\eta^n$ ($n \in \mathbb{Z}$), onde η é a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$. Se $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ contém unidades de norma -1 , então são dadas por $\pm\eta^n$, com n ímpar e, os de norma 1 são dados por $\pm\eta^n$, com n par.*

Como o Teorema 3.6.2 é apenas uma junção dos Teoremas 3.4.6 e 3.5.3, segue o seguinte corolário.

Corolário 3.6.3. *Se $\mathbb{K}$ é um corpo quadrático real, então*

$$U(\mathcal{O}_{\mathbb{K}}) \simeq \mathbb{Z}_2 \times \mathbb{Z}.$$

Agora, apresentamos um resultado análogo ao Teorema 3.4.5, sendo uma consequência do Teorema 3.6.2.

Teorema 3.6.4. *Seja $\mathbb{K}$ um corpo quadrático real. A unidade fundamental de $\mathcal{O}_{\mathbb{K}}$ é a menor unidade de $\mathcal{O}_{\mathbb{K}}$ maior do que 1.*

Demonstração. Seja η a unidade fundamental de $\mathcal{O}_{\mathbb{K}}$ e suponha que existe uma unidade θ de $\mathcal{O}_{\mathbb{K}}$ tal que

$$1 < \theta < \eta.$$

Pelo Teorema 3.6.2, segue que

$$\theta = \pm\eta, \text{ para algum } n \in \mathbb{Z}.$$

Como θ e η são unidades fundamentais, segue que ambos são positivos, e dessa forma, podemos excluir a possibilidade do sinal ser negativo. Assim,

$$\theta = \eta^n.$$

Note que $\eta \geq 1$ ou $\eta \leq 0$. Se $\eta \geq 1$, então

$$\theta = \eta^n \geq \eta.$$

Mas, isso contradiz a hipótese que definimos de $\theta < \eta$. Se $\eta \leq 0$, então

$$\theta = \eta^n \leq 1,$$

o que contradiz que $\theta > 1$. Logo, não existe θ de tal forma, provando que η é a menor unidade maior do que 1. $\square$

O objetivo dessa seção é encontrar a norma da unidade fundamental η de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ para certos valores especiais de m . Mas, antes disso, apresentamos na Tabela 3.1, valores de ϵ (unidade fundamental de norma 1), σ (unidade fundamental de norma -1) e η (unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$), para inteiros positivos m livre de quadrados menores do que 40.

m	ϵ	σ	η	Norma ($N(\eta)$)
2	$3 + 2\sqrt{2}$	$1 + \sqrt{2}$	$1 + \sqrt{2}$	-1
3	$2 + \sqrt{3}$		$2 + \sqrt{3}$	1
5	$(3 + \sqrt{5})/2$	$(1 + \sqrt{5})/2$	$(1 + \sqrt{5})/2$	-1
6	$5 + 2\sqrt{6}$		$5 + 2\sqrt{6}$	1
7	$8 + 3\sqrt{7}$		$8 + 3\sqrt{7}$	1
10	$19 + 6\sqrt{10}$	$3 + \sqrt{10}$	$3 + \sqrt{10}$	-1
11	$10 + 3\sqrt{11}$		$10 + 3\sqrt{11}$	1
13	$11 + 3\sqrt{13}/2$	$(3 + \sqrt{13})/2$	$(3 + \sqrt{13})/2$	-1
14	$15 + 4\sqrt{14}$		$15 + \sqrt{14}$	1
15	$4 + \sqrt{15}$		$4 + \sqrt{15}$	1
17	$33 + 8\sqrt{17}$	$4 + \sqrt{17}$	$4 + \sqrt{17}$	-1
19	$170 + 39\sqrt{19}$		$170 + 39\sqrt{19}$	1
21	$(5 + \sqrt{21})/2$		$(5 + \sqrt{21})/2$	1
22	$197 + 42\sqrt{22}$		$197 + 42\sqrt{22}$	1
23	$24 + 5\sqrt{23}$		$24 + 5\sqrt{23}$	1
26	$51 + 10\sqrt{26}$	$5 + \sqrt{26}$	$5 + \sqrt{26}$	-1
29	$(27 + 5\sqrt{29})/2$	$(5 + \sqrt{29})/2$	$(5 + \sqrt{29})/2$	-1
30	$11 + 2\sqrt{30}$		$11 + 2\sqrt{30}$	1
31	$1520 + 274\sqrt{31}$		$1520 + 273\sqrt{31}$	1
33	$23 + 4\sqrt{33}$		$23 + 4\sqrt{33}$	1
34	$35 + 6\sqrt{34}$		$35 + 6\sqrt{34}$	1
35	$6 + \sqrt{35}$		$6 + \sqrt{35}$	1
37	$73 + 12\sqrt{37}$	$6 + \sqrt{37}$	$6 + \sqrt{37}$	-1
38	$37 + 6\sqrt{38}$		$6 + \sqrt{38}$	1
39	$25 + 4\sqrt{39}$		$25 + 4\sqrt{39}$	1

Tabela 3.1: Unidade fundamental e sua norma em $\mathbb{Q}(\sqrt{m})$

A Tabela 3.1 foi encontrada computacionalmente e calculada na bibliografia [8]. Apesar disso, há outros algoritmos que permitem o cálculo de unidades fundamentais em corpos quadráticos. Na referência [21], há um algoritmo online que calcula a unidade fundamental de corpos quadráticos $\mathbb{Q}(\sqrt{m})$ para $m < 319086769$. Este algoritmo é baseado em [22] (p.382), [23] (p. 62) e [24] (p.359).

A seguir, nosso objetivo é de buscar maneiras de calcular a norma da unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ com generalizações de m . A partir de agora, consideramos m um primo p ímpar. Analisamos o caso $m = p \equiv 1 \pmod{4}$.

Teorema 3.6.5. *Seja p é um primo com $p \equiv 1 \pmod{4}$, então a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ tem norma -1 .*

Este teorema tem duas provas significativas, a primeira é devida a Hilbert e a segunda é devida a Dirichlet. Para este trabalho, a demonstração do Teorema 3.6.5 feita por Dirichlet é mais interessante, uma vez que será replicada de maneira similar na demonstração de outros teoremas a seguir.

Demonstração. (Prova de Dirichlet) Se a unidade fundamental tem norma 1, então

$$\eta = \frac{x + y\sqrt{p}}{2},$$

onde x e y são inteiros positivos tais que

$$x > 2, x \equiv y \pmod{2} \text{ e } x^2 - py^2 = 4.$$

1. Primeiro, vamos analisar o caso em que $x \equiv y \equiv 0 \pmod{2}$. Como ambos são pares pela congruência acima, podemos definir $x = 2X$ e $y = 2Y$, de modo que X e Y são inteiros positivos tais que

$$\eta = X + Y\sqrt{p}, X^2 - pY^2 = 1, X > 1.$$

Como $p \equiv 1 \pmod{4}$, então X é ímpar e Y é par, de modo que $\frac{X-1}{2}$, $\frac{X+1}{2}$ e $\frac{Y}{2}$ são inteiros positivos tais que

$$\frac{X-1}{2} \cdot \frac{X+1}{2} = p \left(\frac{Y}{2} \right)^2. \quad (3.16)$$

Como

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

segue que os inteiros $\frac{X-1}{2}$ e $\frac{X+1}{2}$ são coprimos. Ainda,

$$p \mid \left(\frac{X-1}{2} \right) \cdot \left(\frac{X+1}{2} \right) \Rightarrow p \mid \left(\frac{X-1}{2} \right) \text{ ou } p \mid \left(\frac{X+1}{2} \right).$$

Vamos analisar ambas possibilidades. Se $p \mid \left(\frac{X-1}{2} \right)$, então

$$\frac{X-1}{2p} \cdot \frac{X+1}{2} = \left(\frac{Y}{2} \right)^2.$$

Assim, existem inteiros positivos coprimos A e B tais que

$$\frac{X-1}{2p} = A^2, \frac{X+1}{2} = B^2, \frac{Y}{2} = AB,$$

as quais são as relações a partir da Equação (3.16). Dessa forma,

$$\begin{cases} X = 2pA^2 + 1 = 2B^2 - 1 \\ Y = 2AB. \end{cases}$$

Além disso, $B^2 - pA^2 = 1$, já que

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

Assim, $(B + A\sqrt{p})$ é uma unidade de norma 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$. Agora,

$$\begin{cases} 1 \leq B \leq B^2 \leq 2B^2 - 1 = X \\ 1 \leq A < 2AB = Y. \end{cases}$$

Assim,

$$1 < B + A\sqrt{p} < X + Y\sqrt{p} = \eta,$$

contradizendo que η é a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$. Agora, vamos analisar o segundo caso. Se $p \mid \frac{X+1}{2}$, então

$$\left(\frac{X-1}{2}\right) \cdot \left(\frac{X+1}{2p}\right) = \left(\frac{Y}{2}\right)^2.$$

Portanto, existem inteiros coprimos A e B tais que

$$\frac{X-1}{2} = A^2, \frac{X+1}{2p} = B^2, \frac{Y}{2} = AB.$$

Logo,

$$\begin{cases} X = 2A^2 - 1 = 2pB^2 - 1 \\ Y = 2AB. \end{cases}$$

Consequentemente,

$$A^2 - pB^2 = -1,$$

de modo que $A + B\sqrt{p}$ é uma unidade de norma -1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, contradizendo que todas as unidades de $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ tem norma 1. Assim, fechamos os casos em que $x \equiv y \equiv 0 \pmod{2}$.

2. Vejamos, agora, o caso em que $x \equiv y \equiv 1 \pmod{2}$. Como $p \equiv 1 \pmod{4}$, segue que

$$p = 4k + 1, \text{ com } k \in \mathbb{Z} \Rightarrow 2p = 8k + 2 \Rightarrow$$

$$2p \equiv 2 \pmod{8} \Rightarrow 2p \equiv (\text{mod } 8) \Rightarrow p \equiv 5 \pmod{8}.$$

Logo, $(x-2)$, $(x+2)$ e y são inteiros positivos ímpares tais que

$$(x-2)(x+2) = py^2.$$

Como $(x+2) - (x-2) = 4$, segue que ambos são inteiros coprimos, uma vez que $(x+2)$ e $(x-2)$ são ímpares, e assim, o mdc deles é ímpar e divide $(x-2) - (x+2) = 4$, o que é um absurdo, pois nenhum número ímpar é divisor de 4. Além disso, como $p|(x-2)(x+2)$, então $p|(x-2)$ ou $p|(x+2)$. Novamente, analisamos cada uma das possibilidades. Se $p|(x-2)$, então

$$\frac{(x-2)}{p} \cdot (x+2) = y^2. \quad (3.17)$$

Assim, existem inteiros positivos ímpares A e B , primos entre si, tais que

$$\frac{x-2}{p} = A^2, x+2 = B^2, y = AB.$$

Desse modo,

$$\begin{cases} x = pA^2 + 2 = B^2 - 2 \\ y = AB. \end{cases}$$

Consequentemente, $B^2 - pA^2 = 4$, de modo que $\left(\frac{B + A\sqrt{p}}{2}\right)$ é unidade de norma 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$. Como $B^2 - pA^2 = 4$, segue que $B \neq 1$. Assim, B é ímpar e positivo, e portanto, devemos ter $B \geq 3$. Logo,

$$\begin{cases} 1 < B < B^2 - 2 = x \\ 1 \leq A < AB = y. \end{cases}$$

Assim,

$$2 < \underbrace{B}_{>1} + \underbrace{A}_{>1} \underbrace{\sqrt{p}}_{>1} \Rightarrow 1 < \frac{B + A\sqrt{p}}{2} < \frac{x + y\sqrt{p}}{2}.$$

Mas, isso contradiz o fato que $\left(\frac{x + y\sqrt{p}}{2}\right)$ é a unidade fundamental de norma 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ pelo Teorema 3.4.5. Por outro lado, se $p|(x+2)$, então

$$(x-2) \frac{(x+2)}{p} = y^2.$$

Analogamente, existem inteiros ímpares A, B coprimos tais que

$$x-2 = A^2, \frac{x+2}{p} = B^2, y = AB.$$

Assim,

$$\begin{cases} x = A^2 + 2 = pB^2 - 2 \\ y = AB. \end{cases}$$

Ainda,

$$A^2 - pB^2 = -4.$$

Usando o produto notável, segue que $\left(\frac{A + B\sqrt{p}}{2}\right)$ é uma unidade de norma -1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$, contradizendo o fato que a unidade fundamental tem norma 1.

Assim, garantimos que η tem norma -1 , uma vez que nenhuma possibilidade permite que η seja unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{p})}$ com norma 1 , quando p é primo tal que $p \equiv 1 \pmod{4}$. Portanto, finalizamos a prova do Teorema pelo método de Dirichlet. $\square$

A seguir, precisamos da seguinte definição.

Definição 3.6.6. Seja $p > 1$ um número primo. Dizer que a é um **resto quadrático** de p equivale a dizer que a congruência $x^2 \equiv a \pmod{p}$, onde $p \nmid a$, admite uma solução em $\mathbb{Z}_p$. Notação: aRp . Caso contrário, aNp .

Observação 3.6.7. Se p e q são primos ímpares positivos, $p \nmid q$, $x^2 \equiv p \pmod{q}$ e $x^2 \equiv q \pmod{p}$, então ambas admitem solução ou nenhuma delas admite solução, salvo no caso em que p e q são da forma $4n + 3$, onde neste caso uma admite solução e a outra não.

Definição 3.6.8. O **símbolo de Legendre** é definido por

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{se } p|a; \\ 1, & \text{se } p \nmid a \text{ e } aRp; \\ -1, & \text{se } aNp. \end{cases}$$

Vamos analisar, agora, o caso em que m é divisível por um primo q tal que $q \equiv 3 \pmod{4}$. Veremos que neste caso a unidade fundamental terá norma 1 .

Teorema 3.6.9. *Seja m um inteiro positivo livre de quadrados. Se existe um primo $q \equiv 3 \pmod{4}$ dividindo m , então a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ terá norma 1 .*

Demonstração. Suponha que a unidade fundamental η de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ tem norma -1 . Assim,

$$\eta = \frac{x + y\sqrt{m}}{2},$$

onde x e y são inteiros tais que

$$\begin{cases} x \equiv y \equiv 0 \pmod{2}, & \text{se } m \equiv 2, 3 \pmod{4}; \\ x \equiv y \pmod{2}, & \text{se } m \equiv 1 \pmod{4}. \end{cases}$$

Além disso,

$$\underbrace{\left(\frac{x + y\sqrt{m}}{2}\right)}_{\eta} \cdot \underbrace{\left(\frac{x - y\sqrt{m}}{2}\right)}_{\text{conjugado de } \eta} = \frac{x^2 - my^2}{4} = N(\eta) = -1 \Rightarrow x^2 - my^2 = -4.$$

Como $q|m$ por hipótese, segue que

$$x^2 \equiv -4 \pmod{q}.$$

Portanto,

$$\left(\frac{-4}{q}\right) = 1.$$

Mas, se $m \equiv 2, 4 \pmod{4}$, então $x^2 - my^2 = -1$. Como $q|m$, segue que

$$\left(\frac{-1}{q}\right) = 1.$$

Logo, $\left(\frac{-4}{q}\right) = \left(\frac{-1}{q}\right)$, o que implica $q \equiv 1 \pmod{4}$, contradizendo que $q \equiv 3 \pmod{4}$. Isso prova que η deve ter norma 1 . $\square$

Teorema 3.6.10. *Se p é um primo com $p \equiv 5 \pmod{8}$, então a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{2p})}$ tem norma -1 .*

Demonstração. Se $m = 2p$, então

$$\begin{aligned} p \equiv 5 \pmod{8} &\Rightarrow 2p \equiv 10 \pmod{8} \Rightarrow m \equiv 2 \pmod{8} \\ &\Rightarrow m - 2 \mid 8 \Rightarrow m - 2 = 8k, \text{ com } k \in \mathbb{Z} \Rightarrow m = 8k + 2 \\ &\Rightarrow m = 4(2k) + 2 \Rightarrow m \equiv 2 \pmod{4}. \end{aligned}$$

Suponha que a unidade fundamental tem norma 1. Assim, pela Definição 3.4.3, segue que

$$\eta = x + y\sqrt{2p} \Rightarrow \eta = x + y\sqrt{m}$$

tal que

$$x > 1 \text{ e } x^2 - my^2 = 1.$$

Agora, como $p \equiv 5 \pmod{8}$, segue que $p \equiv 1 \pmod{4}$. Logo, se x é par, então y é ímpar. Assim, sejam $(x-1)$, $(x+1)$ e y inteiros positivos ímpares tais que

$$(x-1)(x+1) = my^2,$$

ou seja,

$$x^2 - 1 = my^2 \Rightarrow x^2 - my^2 = 1 \Rightarrow (x - \sqrt{m}y) \underbrace{(x + \sqrt{m}y)}_{\epsilon} = 1.$$

Como $(x+1) - (x-1) = x - x - 1 + 1 = 1$, segue que $(x-1)$ e $(x+1)$ são primos entre si. Como $m \mid (x-1)(x+1)$, segue que $2p \mid (x-1)(x+1)$. Mas, ambos são ímpares, e portanto, $2 \nmid (x-1)(x+1)$. Assim,

$$p \mid \frac{(x-1)}{2} \quad \text{ou} \quad p \mid \frac{(x+1)}{2},$$

e deste modo,

$$(x-1)(x+1) = 2py^2 \Rightarrow \frac{(x-1)(x+1)}{2p} = y^2.$$

Analisamos os dois possíveis casos. Se $p \mid \frac{(x-1)}{2}$, então existe $A, B \in \mathbb{Z}_+$, $\text{mdc}(a, b) = 1$, tais que

$$\frac{x-1}{2p} = A^2, \quad x+1 = B^2 \quad \text{e} \quad y = AB.$$

Assim,

$$\begin{cases} x = 2pA^2 + 1 = B^2 - 1 \\ y = AB. \end{cases}$$

Como $\underbrace{B^2}_{>0} - (2p)A^2 = 1$, segue que $B + A\sqrt{2p}$ é uma unidade de norma 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{2p})}$.

Além disso

$$\begin{cases} 1 \leq B \leq B^2 - 1 = x \\ 1 \leq A < AB - y \end{cases} \Rightarrow 1 \leq B + A \underbrace{\sqrt{2p}}_{>1} < x + y\sqrt{2p} = \eta,$$

ou seja, existe uma unidade maior do que 1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{2p})}$ menor do que a unidade fundamental, contradizendo o Teorema 3.6.4. Agora, se $p \mid \frac{(x+1)}{2}$, então

$$(x-1) \cdot \frac{(x+1)}{2p} = y^2.$$

Assim, existe $A, B \in \mathbb{Z}_+$, $\text{mdc}(A, B) = 1$, tais que

$$x-1 = A^2, \frac{x+1}{2p} = B^2, y = AB.$$

Desse modo,

$$\begin{cases} x = A^2 + 1 = 2pB^2 - 1 \\ y = AB. \end{cases}$$

Logo,

$$A^2 - 2pB^2 = -1 \Rightarrow (A - \sqrt{2p}B)(A + \sqrt{2p}B) = -1,$$

ou seja, $A + \sqrt{2p}B$ é uma unidade de norma -1 em $\mathcal{O}_{\mathbb{Q}(\sqrt{2p})}$, contradizendo nossa hipótese inicial de que todas as unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{2p})}$ tem norma 1. Portanto, para p primo tal que $p \equiv 5 \pmod{8}$, segue que a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{2p})}$ tem norma -1 . $\square$

Teorema 3.6.11. *Se p e q são primos distintos tais que*

$$p \equiv q \equiv 1 \pmod{4}, \left(\frac{p}{q}\right) = -1,$$

então a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{pq})}$ tem norma -1 .

Demonstração. Suponha que a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{pq})}$ tem norma 1. Assim,

$$\begin{cases} p \equiv 1 \pmod{4} \\ q \equiv 1 \pmod{4} \end{cases} \Rightarrow pq \equiv 1 \pmod{4}.$$

Logo,

$$\eta = \frac{x + y\sqrt{pq}}{2},$$

onde x, y são inteiros positivos tais que $x > 2$, $x \equiv y \pmod{2}$, $x^2 - (pq)y^2 = 4$. Vamos primeiro analisar o caso em que $x \equiv y \pmod{2}$. Defina $X = \frac{x}{2}$ e $Y = \frac{y}{2}$, de modo que X, Y são os menores inteiros positivos tais que

$$X > 1, \eta = X + Y\left(\sqrt{PQ}\right), X^2 - (pq)Y^2 = 1.$$

Como $pq \equiv 1 \pmod{4}$, então $pq \equiv 1 \pmod{2}$. Dessa forma, X é ímpar se, e somente se, Y é par e vice-versa, uma vez que

1. se Y é par, então

$$1 \equiv 1 \pmod{2} \Leftrightarrow X^2 - (pq)Y^2 \equiv 1 \pmod{2} \Leftrightarrow X^2 \equiv 1 + (pq)Y^2 \pmod{2} \stackrel{Y \text{ par}}{\Leftrightarrow}$$

$$X^2 \equiv 1 \pmod{2} \Leftrightarrow X \equiv 1 \pmod{2}.$$

Portanto, X é ímpar.

2. Por outro lado, se X par, então

$$\begin{aligned} X^2 &\equiv 1 + (pq)Y^2 \pmod{2} \Leftrightarrow 0 \equiv 1 + (pq)Y^2 \pmod{2} \Leftrightarrow \\ &\underbrace{(pq)}_{\equiv 1 \pmod{2}} Y^2 \equiv 1 \pmod{2} \Leftrightarrow Y \equiv 1 \pmod{2}. \end{aligned}$$

Portanto, Y é ímpar.

Assim, seja X ímpar e Y par, então $\frac{X-1}{2}$, $\frac{X+1}{2}$ e $\frac{Y}{2}$ são inteiros positivos tais que

$$\frac{(X-1)}{2} \cdot \frac{(X+1)}{2} = (pq) \left(\frac{Y}{2}\right)^2.$$

Como $\frac{(X-1)}{2} - \frac{(X+1)}{2} = 1$, então os inteiros $\frac{(X-1)}{2}$, $\frac{(X+1)}{2}$ são coprimos. Logo,

$$pq \left| \frac{(X-1)}{2} \cdot \frac{(X+1)}{2} \right|.$$

Assim, obtemos as quatro seguintes possibilidades:

$$pq \left| \frac{(X-1)}{2}; \quad pq \left| \frac{(X+1)}{2}; \quad p \left| \frac{(X-1)}{2} \text{ e } q \left| \frac{(X+1)}{2}; \quad q \left| \frac{(X-1)}{2} \text{ e } p \left| \frac{(X+1)}{2} \right|.$$

Analisamos cada uma dessas.

1. Se $pq \left| \frac{(X-1)}{2}$, então

$$\frac{X-1}{2pq} \cdot \frac{X+1}{2} = \left(\frac{Y}{2}\right)^2,$$

e assim, existe $A, B \in \mathbb{Z}_+$ com $\text{mdc}(A, B) = 1$ tais que

$$\frac{X-1}{2pq} = A^2, \quad \frac{X+1}{2} = B^2, \quad \frac{Y}{2} = AB.$$

Daí, $X = 2pqA^2 + 1 = 2B^2 - 1$ e $Y = 2AB$. Agora,

$$\frac{X-1}{2} - \frac{X+1}{2} = 1 \Rightarrow \frac{X-1}{2} - \frac{pq}{2} \frac{X+1}{2} = 1 \Rightarrow B^2 - pqA^2 = 1.$$

Logo, $B + A\sqrt{pq}$ é uma unidade de $\mathcal{O}_{Q(\sqrt{pq})}$. Note que

$$\begin{cases} 1 \leq B \leq B^2 \leq 2B^2 - 1 = X \\ 1 \leq A < 2AB = Y. \end{cases}$$

Assim, $B + A\sqrt{pq} < x + y\sqrt{pq} = \eta$, o que é um absurdo pelo Teorema 3.6.4.

2. Seja $pq \left| \frac{(X+1)}{2}$. De maneira análoga, segue que existe uma unidade de $\mathcal{O}_{Q(\sqrt{pq})}$ que tem norma -1 , contradizendo a hipótese.

3. Se $p \mid \frac{(X-1)}{2}$ e $q \mid \frac{(X+1)}{2}$, então

$$\frac{X-1}{2p} \cdot \frac{X+1}{2q} = \left(\frac{Y}{2}\right)^2.$$

Considerando

$$A = \frac{X-1}{2p}, \quad B = \frac{X+1}{2q},$$

com $A, B \in \mathbb{Z}_+$ coprimos, segue que

$$qB^2 - pA^2 = 1.$$

Assim,

$$qB^2 \equiv 1 \pmod{p} \Rightarrow B \not\equiv 0 \pmod{p} \Rightarrow q \equiv \left(\frac{1}{B}\right) \pmod{p},$$

o que é um absurdo, uma vez que $\left(\frac{p}{q}\right) = -1$.

4. Se $1 \mid \frac{(X-1)}{2}$ e $p \mid \frac{(X+1)}{2}$, então

$$\frac{X-1}{2q} \cdot \frac{X+1}{2p} = \left(\frac{Y}{2}\right)^2.$$

Sejam $A, B \in \mathbb{Z}_+$ coprimos tais que

$$A = \frac{X-1}{2p}, \quad B = \frac{X+1}{2q}.$$

Dessa forma,

$$pB^2 - qA^2 = 1.$$

Logo, segue que

$$pB^2 \equiv 1 \pmod{q}.$$

Assim,

$$B \not\equiv 0 \pmod{q} \Rightarrow p \equiv \left(\frac{1}{B}\right)^2 \pmod{q},$$

Mas, isso contradiz a hipótese de que $\left(\frac{p}{q}\right) = -1$,

o que prova o resultado. $\square$

Uma consequência direta do Teorema 3.3.1 é que se m é um inteiro, então existe uma quantidade infinita de soluções com $x \equiv 0 \pmod{m}$. No estudo das unidades em corpos quadráticos $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, vimos que a equação de Pell toma a forma $y^2 - mx^2 = 4$.

Se $(x, y) = (X, Y)$, $X > 0$, $Y > 0$ é a solução com o menor x , então a solução geral será dada por

$$\frac{x + y\sqrt{d}}{2} = \pm \left(\frac{X + Y\sqrt{m}}{2}\right)^n, \quad \text{onde } n \in \mathbb{Z}.$$

Vimos que a solução da equação $x^2 - my^2 = -1$, isto é, a norma da unidade fundamental é -1, é uma questão mais complicada e não há condições explícitas para sua

solubilidade. Uma condição necessária é que m não seja divisível por 4 ou por nenhum primo $p \equiv 3 \pmod{4}$. Mas, a equação tem solução para $m = p$ primo tal que $p \equiv 1 \pmod{4}$. Assim, considere $(x, y) = (X, Y)$ a solução fundamental de $x^2 - my^2 = 1$. Desse modo, $X \equiv 1, Y \equiv 0 \pmod{2}$. Assim, tomando

$$\frac{X+1}{2} \cdot \frac{X-1}{2} = p \left(\frac{Y}{2} \right)^2,$$

então, para A, B inteiros positivos,

$$1. \quad \frac{X+1}{2} = pA^2, \quad \frac{X-1}{2} = B^2 \text{ ou}$$

$$2. \quad \frac{X+1}{2} = A^2, \quad \frac{X-1}{2} = pB^2.$$

Observe que o item 2, implica que $A^2 - pB^2 = 1$ e contradiz que a unidade fundamental tem norma -1. Agora, o item 1, nos dá $B^2 - pA^2 = -1$. Assim, existe uma quantidade infinita de soluções dadas por

$$x + y\sqrt{m} = (B + A\sqrt{p})^{2n+1}, \text{ onde } n \in \mathbb{Z}.$$

A solução fundamental X, Y é acima é dada de maneira direta por

$$X + Y\sqrt{p} = (B + A(\sqrt{p}))^2.$$

Dessa forma, a equação de Pell volta a ser objeto de estudo para as unidades de corpos quadráticos $\mathbb{Q}(\sqrt{m})$, onde $m > 0$ é inteiro livre de quadrados. Na Definição 3.4.3, juntamente com o Teorema 2.4.9, vimos que

$$m \equiv 2, 3 \pmod{4} \Rightarrow \eta = x + y\sqrt{d}, \quad x^2 - my^2 = 1$$

$$m \equiv 1 \pmod{4} \Rightarrow \eta = x + \left(\frac{1 + \sqrt{m}}{2} \right) y, \quad x^2 + xy + \left(\frac{1 - m}{4} \right) y^2 = \pm 1,$$

onde x, y são racionais. E, pelo Teorema 3.5.3, vimos como a unidade fundamental de norma -1 se relaciona com a de norma 1. Ambas equações satisfazem a forma $X^2 - mY^2 = \pm 4$ e, claramente, a unidade fundamental η é a solução com os menores inteiros positivos X e Y .

3.7 Calculando a unidade fundamental

Apesar de termos feito alguns casos de como calcular a unidade fundamental de certos corpos quadráticos reais, ainda não apresentamos formalmente como calcular a unidade fundamental η para um corpo quadrático $\mathbb{Q}(\sqrt{m})$, para m um inteiro positivo livre de quadrados qualquer. Este problema será desenvolvido nesta seção, em que apresentamos um método padrão de calcular a unidade fundamental η de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$, por meio de expansão da fração contínua de $\sqrt{m}$, com m inteiro positivo livre de quadrados. Desta maneira, generalizamos como encontrar as unidades dos corpos reais $\mathbb{K} = \mathbb{Q}(\sqrt{m})$. Para isso, relembremos conceitos de frações contínuas.

Definição 3.7.1. Sejam $x_0, x_1, x_2, \dots \in \mathbb{Z}$, com $x_1, x_2, \dots > 0$. Uma sequência da forma

$$x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \frac{1}{\ddots}}}}$$

é chamada **fração contínua simples**. Os números $x_0, x_1, x_2, \dots \in \mathbb{Z}$ são chamadas quocientes parciais. Se o número de x_i 's é finito, a fração contínua é dita finita. Caso contrário, é dita infinita.

Definição 3.7.2. Uma fração contínua simples é **periódica** se sua expressão tem a forma $[x_0; x_1, x_2, \dots, y_0, y_1, \dots, y_t, y_0, y_1, \dots, y_t, \dots]$.

Observação 3.7.3. Denotamos a fração contínua $x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \frac{1}{\ddots}}}}$ por $[x_0; x_1, x_2, x_3, \dots]$.

Se for periódica, denotamos por $[x_0; x_1, x_2, x_3, \dots, \overline{y_0, y_1, \dots, y_t, \dots}]$.

Nosso objetivo é trabalhar com o número irracional $\sqrt{m}$, onde m inteiro positivo livre de quadrados. Para isso, definimos a sequência $x_0, x_1, x_2, \dots$ de números reais, por

$$x_0 = \sqrt{m} \text{ e } x_{n+1} = \frac{1}{x_n - [x_n]}, \quad n = 0, 1, 2, \dots \quad (3.18)$$

onde $[x_n]$ denota o maior inteiro que é menor ou igual a x_n .

Observação 3.7.4. Note que claramente cada $x_n > 1$ e podemos reescrever como

$$x_n = \frac{P_n + \sqrt{m}}{Q_n}, \quad n = 0, 1, 2, \dots$$

onde $P_0 = 0$, $Q_0 = 1$ e P_n, Q_n são inteiros positivos para $n \geq 1$.

Para frações contínuas infinitas periódicas, existe um inteiro l positivo tal que $x_{l+1} = x_1$. Pela Equação (3.18), segue que $x_{l+2} = x_2, x_{l+3} = x_3, \dots$, de modo que a sequência $\{x_n\}_{n \geq 1}$ é puramente periódica.

Defina

$$y_n = [x_n], \text{ com } n = 0, 1, 2, \dots,$$

de modo que $\{x_n\}_{n \geq 1}$ é uma sequência de inteiros positivos. Como $\{x_n\}_{n \geq 1}$ é uma sequência puramente periódica, segue que $\{y_n\}_{n \geq 1}$ também é uma sequência puramente periódica.

Exemplo 3.7.5. Se $m = 31$, a expansão em fração contínua de $\sqrt{31}$ é dada por

$$\begin{aligned}
x_0 &= \sqrt{31}, \\
x_1 &= \frac{1}{x_0 - [x_0]} = \frac{1}{\sqrt{31} - 5} = \frac{5 + \sqrt{31}}{6}, \\
x_2 &= \frac{1}{x_1 - [x_1]} = \frac{1}{\frac{5 + \sqrt{31}}{6} - 1} = \frac{1 + \sqrt{31}}{5}, \\
x_3 &= \frac{1}{x_2 - [x_2]} = \frac{1}{\frac{1 + \sqrt{31}}{5} - 1} = \frac{4 + \sqrt{31}}{3}, \\
x_4 &= \frac{1}{x_3 - [x_3]} = \frac{1}{\frac{4 + \sqrt{31}}{3} - 3} = \frac{5 + \sqrt{31}}{2}, \\
x_5 &= \frac{1}{x_4 - [x_4]} = \frac{1}{\frac{5 + \sqrt{31}}{2} - 5} = \frac{5 + \sqrt{31}}{3}, \\
x_6 &= \frac{1}{x_5 - [x_5]} = \frac{1}{\frac{5 + \sqrt{31}}{3} - 3} = \frac{4 + \sqrt{31}}{5}, \\
x_7 &= \frac{1}{x_6 - [x_6]} = \frac{1}{\frac{4 + \sqrt{31}}{5} - 1} = \frac{1 + \sqrt{31}}{6}, \\
x_8 &= \frac{1}{x_7 - [x_7]} = \frac{1}{\frac{1 + \sqrt{31}}{6} - 1} = \frac{5 + \sqrt{31}}{1}, \\
x_9 &= \frac{1}{x_8 - [x_8]} = \frac{1}{\frac{5 + \sqrt{31}}{1} - 10} = \frac{5 + \sqrt{31}}{6} = x_1,
\end{aligned}$$

Continuando com esse processo, segue que $x_{10} = x_2$, $x_{11} = x_3, \dots$, ou seja, é uma fração contínua periódica. Mais ainda, $\{y_n\}_{n \geq 0} = \{5, 1, 1, 3, 5, 3, 1, 1, 10, 1, 1, 3, 5, 3, 1, 1, 10, \dots\}$

A seguir, vamos definir duas outras sequências, que serão úteis.

Definição 3.7.6. Sejam $y_0, y_1, y_2, \dots$ uma sequência infinita de inteiros, todos positivos (exceto por talvez x_0). Definimos duas sequências de inteiros $\{h_n\}_{n \geq -1}$ e $\{k_n\}_{n \geq -1}$ indutivamente por:

- $h_{-1} = 1$, $h_0 = y_0$, $h_n = y_n h_{n-1} + h_{n-2}$, $n = 1, 2, \dots$
- $k_{-1} = 0$, $k_0 = 1$, $k_n = y_n k_{n-1} + k_{n-2}$, $n = 1, 2, \dots$

Observação 3.7.7. Todos os h_n e k_n são positivos, exceto para $k_{-1} = 0$. Além disso,

$$k_0 = 1, k_1 = x_1 k_0 \geq k_0, k_2 > k_1, k_3 > k_2, \text{ etc.}$$

Dessa forma, $1 = k_0 \geq k_1 < k_2 < k_3 < \dots < k_n < \dots$

Teorema 3.7.8. Se y é um número real positivo, então

$$[y_0; y_1, \dots] = \frac{y h_{n-1} + h_{n-2}}{y k_{n-1} + k_{n-2}}.$$

Demonstração. A prova será por indução sobre n . Se $n = 0$, então

$$y = \frac{yh_{-1} + h_{-2}}{yk_{-1} + k_{-2}} \stackrel{3.7.6}{=} \frac{y \cdot 1 + 0}{y \cdot 0 + 1} = \frac{y}{1}.$$

Se $n = 1$, então

$$[y_0, y] = \frac{yh_0 + h_{-1}}{yk_0 + k_{-1}} \Rightarrow y_0 + \frac{1}{y} = \frac{y(y_0h_{-1} + h_{-2}) + 1}{y(y_0 \cdot y_{-1}) + y_{-2}} = \frac{y(y_0) + 1}{y \cdot (1) + 0} = \frac{y(y_0)}{y} + \frac{1}{y} = y_0 + \frac{1}{y},$$

e assim, a igualdade se verifica. Agora, considere que o resultado vale para $[y_0, y_1, \dots, y_{n-1}, y]$. Logo,

$$\begin{aligned} [y_0, y_1, \dots, y_n, x] &= \left[y_0, y_1, \dots, y_n + \frac{1}{y} \right] = \frac{(y_n + \frac{1}{y})h_{n-1} + h_{n-2}}{(y_n + \frac{1}{y})k_{n-1} + k_{n-2}} \\ &= \frac{y(y_nh_{n-1} + h_{n-2}) + h_{n-1}}{y(y_nk_{n-1} + k_{n-2}) + k_{n-1}} = \frac{yh_n + h_{n-1}}{yk_n + k_{n-1}}, \end{aligned}$$

ou seja, provamos que o resultado vale para n , como queríamos. $\square$

Teorema 3.7.9. Se $r_n = [y_0, y_1, \dots, y_n]$ para todos inteiros $n \geq 0$, então $r_n = \frac{h_n}{k_n}$.

Demonstração. Basta aplicar o Teorema 3.7.8 com x substituído por x_n e usar a Definição 3.7.6, e assim,

$$r_n = [y_0, y_1, \dots, y_n] = \frac{y_nh_{n-1} + h_{n-2}}{y_nk_{n-1} + k_{n-2}} = \frac{h_n}{k_n},$$

o que prova o resultado. $\square$

Teorema 3.7.10. Se $n \geq 1$ é um inteiro, então

$$h_nk_{n-1} - h_{n-1}k_n = (-1)^{n-1} \quad e \quad r_n - r_{n-1} = \frac{(-1)^{n-1}}{k_nk_{n-1}}.$$

Além disso, a fração $\frac{h_i}{k_i}$ é reduzida, isto é, $\text{mdc}(h_i, k_i) = 1$.

Demonstração. A prova será por indução sobre n . Pela Definição 3.7.6, segue que

$$h_{-1}k_{-2} - h_{-2}k_{-1} = 1.$$

Agora suponha que a equação é válida para $h_{n-1}k_{n-2} - h_{n-2}k_{n-1} = (-1)^{n-2}$. Novamente, pela Definição 3.7.6, segue que

$$\begin{aligned} h_nk_{n-1} - h_{n-1}k_n &= (y_nh_{n-1} + h_{n-2})k_{n-1} - h_{n-1}(y_nk_{n-1} + k_{n-2}) \\ &= \cancel{y_nh_{n-1}k_{n-1}} + h_{n-2}k_{n-1} - \cancel{h_{n-1}y_nk_{n-1}} - h_{n-1}k_{n-2} \\ &= -(h_{n-1}k_{n-2} - h_{n-2}k_{n-1}) = (-1)(-1)^{n-2} = (-1)^{n-1}. \end{aligned}$$

Isso prova a primeira equação do Teorema. Para a segunda equação, basta dividir a primeira por $k_{n-1}k_n$, uma vez que

$$r_n - r_{n-1} = \frac{h_n}{k_n} - \frac{h_{n-1}}{k_{n-1}} = \frac{h_nk_{n-1} - h_{n-1}k_n}{k_n \cdot k_{n-1}} \Rightarrow r_n - r_{n-1} = \frac{(-1)^{n-1}}{k_{n-1}k_n}.$$

Por fim, a fração $\frac{h_n}{k_n}$ está sem seus menores termos, já que cada fator de h_n e k_n é também um fator de $(-1)^{n-1}$. Logo, podemos concluir que $\text{mdc}(h_n, k_n) = 1$. $\square$

Observação 3.7.11. O limite $\lim_{n \rightarrow \infty} r_n$ existe, pois considerando a sequência infinita dos $r_0, r_1, r_2, \dots$, segue que os elementos de índice par $r_0, r_2, r_4, \dots, r_{2j}, (j \in \mathbb{N})$, dessa sequência formam uma sequência monótona crescente e os elementos de índice ímpares $r_1, r_3, \dots, r_{2j+1}, (j \in \mathbb{N})$, foram uma sequência monótona decrescente. Ambas subsequências são limitadas, e portanto, podemos garantir que o limite existe. Além disso, ambos limites são iguais, uma vez que $r_n - r_{n-1}$ tende para zero quando n tende para infinito, já que os inteiros k_n estão crescendo junto com n .

Definição 3.7.12. Um sequência infinita $y_0, y_1, y_2, \dots$ de inteiros, todos positivos exceto por talvez y_0 , determina uma **fração contínua simples infinita** $[y_0; y_1, y_2, \dots]$. O valor de $[y_0; y_1, y_2, \dots]$ é definido por $\lim_{n \rightarrow \infty} [y_0; y_1, y_2, \dots, y_n]$, isto é,

$$[y_0; y_1, y_2, \dots] = \lim_{n \rightarrow \infty} [y_0; y_1, y_2, \dots, y_n].$$

Pela Definição 3.7.12, segue que $\sqrt{m}$ possui a expansão em fração contínua infinita dada por

$$[y_0; y_1, y_2, \dots] = \sqrt{m}. \quad (3.19)$$

Este limite é o mesmo que $\lim_{n \rightarrow \infty} r_n$, que já vimos que existe na Observação 3.7.11. Outra forma de escrever esse limite é $\lim_{n \rightarrow \infty} \frac{h_n}{k_n}$.

Assim, como já havíamos mencionado, a sequência $\{x_n\}_{n \geq 1}$ é puramente periódica. Agora, se l é o menor inteiro positivo tal que $x_{l+n} = x_n$ (equivalentemente, $P_{l+n} = P_n$, $Q_{l+n} = Q_n$ para todos inteiros positivos n , então o inteiro l é dito período da expansão em fração contínua de $\sqrt{m}$. Assim,

$$\sqrt{m} = [y_0, y_1, \dots, y_l, y_1, \dots, y_l, y_1, \dots, y_l, \dots]$$

pode ser abreviado por

$$\sqrt{m} = [y_0, \overline{y_1, \dots, y_l}].$$

Exemplo 3.7.13. Para $m = 31$, segue que

$$\{h_n\}_{n \geq -1} = \{1, 5, 6, 11, 96, 206, 657, 863, 1520, 16063, 17583, \dots\}$$

$$\{k_n\}_{n \geq -1} = \{0, 1, 1, 2, 7, 37, 118, 155, 273, 1885, 3158, \dots\}.$$

Agora, calculamos os valores de $r_n = \frac{h_n}{k_n}$ para encontrar o valor de $\sqrt{31}$.

$$\begin{array}{lll} \frac{h_0}{k_0} = \frac{5}{1} = 5, & \frac{h_1}{k_1} = \frac{6}{1} = 6, & \frac{h_2}{k_2} = \frac{11}{2} = 5.5, \\ \frac{h_3}{k_3} = \frac{39}{7} = 5.5714285, & \frac{h_4}{k_4} = \frac{206}{37} = 5.5675675, & \frac{h_5}{k_5} = \frac{657}{118} = 5.5677966, \\ \frac{h_6}{k_6} = \frac{863}{155} = 5.5677419, & \frac{h_7}{k_7} = \frac{1520}{273} = 5.5677655, & \frac{h_8}{k_8} = \frac{16063}{2885} = 5.5677642, \\ \frac{h_9}{k_9} = \frac{17583}{3158} = 5.5677644. & & \end{array}$$

E $\sqrt{31} = 5.5677643 \dots$. Note que os valores encontrados tem aproximação de sete casas decimais. Ainda, $l = 8$, e portanto,

$$\sqrt{31} = [5, 1, 1, 3, 5, 3, 1, 1, 10, 1, 1, 3, 5, 3, 1, 1, 10, 1, \dots] = [5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$$

Observamos que $y_0 = [\sqrt{m}]$ e $x_l = 2x_0$. Colocando

$$x_n = \frac{P_n + \sqrt{m}}{Q_n}, \quad x_{n-1} = \frac{P_{n-1} + \sqrt{m}}{Q_{n-1}},$$

e $[x_{n-1}] = y_{n-1}$ em

$$x_n = \frac{1}{x_{n-1} - [x_{n-1}]}, \quad \text{para } n \geq 1,$$

segue que

$$\frac{P_n + \sqrt{m}}{Q_n} = \frac{Q_{n-1}}{(P_{n-1} - y_{n-1}Q_{n-1}) + \sqrt{m}}.$$

Multiplicando cruzado e igualando os coeficientes, segue que

$$\begin{cases} P_n(P_{n-1} - y_{n-1}Q_{n-1}) + m = Q_nQ_{n-1}, \\ P_n + P_{n-1} - y_{n-1}Q_{n-1} = 0. \end{cases}$$

Portanto, $x_n = \frac{P_n + \sqrt{m}}{Q_n}$, para $n \geq 1$, é determinada recursivamente por

$$\begin{aligned} P_n &= -P_{n-1} + y_{n-1}Q_{n-1}, \\ Q_n &= \frac{m - P_n^2}{Q_{n-1}}, \\ y_n &= \left[\frac{P_n + \sqrt{m}}{Q_n} \right], \end{aligned}$$

com $P_0 = 0$, $Q_0 = 1$ e $y_0 = [\sqrt{m}]$.

O resultado principal que permite determinar a unidade fundamental de um corpo real quadrático é dado pelo seguinte teorema.

Teorema 3.7.14. [8] *Seja m um inteiro positivo livre de quadrados. Sejam h_n/k_n , onde $n = 0, 1, 2, \dots$, os convergentes da expansão da fração contínua infinita de $\sqrt{m}$. Seja l o período da expansão.*

1. *Se l é par, então $x^2 - my^2 = -1$ não tem solução em inteiros x e y e a solução de $x^2 - my^2 = 1$ em inteiros positivos x e y com x sendo o menor é $(x, y) = (h_{l-1}, k_{l-1})$.*
2. *Se l é ímpar, então $x^2 - my^2 = -1$ tem solução em inteiros x e y e a solução de $x^2 - my^2 = -1$ em inteiros positivos x e y com x sendo o menor é dada por $(x, y) = (h_{l-1}, k_{l-1})$.*

Com base nesses resultados, obtemos alguns casos que vão diferenciar qual a unidade do anel $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$.

1. Se $m \equiv 2$, $m \equiv 3 \pmod{4}$ ou $m \equiv 1 \pmod{8}$ todas as unidades de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ são da forma $x + y\sqrt{m}$, com x e y inteiros. Assim, pelos Teoremas 3.6.4 e 3.7.14, segue que a unidade fundamental η de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ é dada por

$$\eta = h_{l-1} + k_{l-1}\sqrt{m}, \quad N(\eta) = (-1)^l.$$

2. Se $m \equiv 5 \pmod{8}$ pode ou não existir unidades de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ da forma $\frac{1}{2}(x + y\sqrt{m})$ com x e y inteiros ímpares. Se não existe tal unidade, então $\eta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ e, como no item 1, segue que

$$\eta = h_{l-1} + k_{l-1}\sqrt{m}, \quad N(\eta) = (-1)^l.$$

Se essas unidades existem, então $\eta \notin \mathbb{Z} + \mathbb{Z}\sqrt{m}$ e pode-se mostrar que $\eta^3 \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Nesse caso, $\eta^3 = x + y\sqrt{m}$, onde x e y são inteiros positivos satisfazendo $x^2 - my^2 = \pm 1$ com x sendo o menor. Assim, pelos Teoremas 3.6.4 e 3.7.14,

$$\eta = h_{l-1} + k_{l-1}\sqrt{m}, \quad N(\eta) = (-1)^l.$$

Se $\eta = \frac{A + B\sqrt{m}}{2}$, onde A e B são inteiros ímpares positivos, então

$$\left(\frac{A + B\sqrt{m}}{2}\right)^2 = h_{l-1} + k_{l-1}\sqrt{m},$$

e portanto,

$$\begin{aligned} A^3 + 3AB^2m &= 8h_{l-1}, \\ 3A^2B + B^3m &= 8k_{l-1}. \end{aligned}$$

Consequentemente,

$$\begin{aligned} A &\mid h_{l-1}, \quad 1 \leq A < 2(h_{l-1})^{1/3}, \\ B &\mid k_{l-1}, \quad 1 \leq B < 2\left(\frac{k_{l-1}}{m}\right)^{1/3}. \end{aligned}$$

Com isso, apresentamos o seguinte algoritmo para determinar a unidade fundamental η de $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ para um inteiro positivo livre de quadrados m .

Algoritmo.

Passo 1: Considere os valores

$$h_{-1} = 1, \quad k_{-1} = 0, \quad P_0 = 0, \quad Q_0 = 1, \quad y_0 = \lfloor \sqrt{m} \rfloor, \quad h_0 = \lfloor \sqrt{m} \rfloor, \quad k_0 = 1.$$

Passo 2: Determine P_n, Q_n, y_n, h_n, k_n ($n = 1, 2, \dots$) recursivamente, para $n = 1, 2, \dots$,

$$\begin{aligned} P_n &= -P_{n-1} + y_n - 1Q_{n-1}, \\ Q_n &= \frac{m - P_n^2}{Q_{n-1}}, \\ y_n &= \left\lfloor \frac{P_n + \sqrt{m}}{Q_n} \right\rfloor \\ h_n &= a_n h_{n-1} + h_{n-2} \\ k_n &= y_n k_{n-1} + k_{n-2}. \end{aligned}$$

Pare esse processo no primeiro inteiro $N > 1$ tal que

$$P_N = P_1 \quad \text{e} \quad Q_N = Q_1.$$

Passo 3: Considere $l = N - 1$.

Passo 4: Se $m \equiv 2 \pmod{4}$, $m \equiv 3 \pmod{4}$ ou $m \equiv 1 \pmod{8}$, então

$$\eta = h_{l-1} + k_{l-1}\sqrt{m}, \quad N(\eta) = (-1)^l.$$

Passo 5: Se $m \equiv 5 \pmod{4}$, então determine todos os divisores positivos ímpares A de h_{l-1} menores do que $2(h_{l-1})^{1/3}$ e todos os divisores positivos pares B de k_{l-1} menores do que $2(k_{l-1}/m)^{1/3}$. Se para algum par (A, B) tivermos

$$\begin{aligned} A^3 + 3AB^2m &= 8h_{l-1}, \\ 3A^2B + B^3m &= 8k_{l-1}, \end{aligned}$$

então

$$\eta = \frac{A + B\sqrt{m}}{2}, \quad N(\eta) = (-1)^l;$$

Caso contrário,

$$\eta = h_{l-1} + k_{l-1}\sqrt{m}, \quad N(\eta) = (-1)^l.$$

Primeiramente, vamos aplicar o algoritmo para o caso em que $m = 31$. Em seguida, apresentamos outros possíveis casos.

Exemplo 3.7.15. Para $m = 31$, segue que

$$m = 31 \equiv 3 \pmod{4}.$$

Começando com $h_{-1} = 1, k_{-1} = 0, P_0 = 0, Q_0 = 1, y_0 = 5, h_0 = 5, k_0 = 1$, obtemos sucessivamente os valores de P_n, Q_n, y_n, h_n, k_n , para $n = 1, 2, \dots$, como no passo 2.

n	P_n	Q_n	y_n	h_n	k_n
-1				1	0
0	0	1	5	5	1
1	5	6	1	6	1
2	1	5	1	11	2
3	4	3	3	39	7
4	5	2	5	206	37
5	5	3	3	657	118
6	4	5	1	863	155
7	1	6	1	1520	273
8	5	1	10	16063	2885
9	5	6	1	17583	3158

Como $P_9 = P_1 = 5$ e $Q_9 = Q_1 = 6$, segue que

$$N = 9, l = N - 1 = 8, h_{l-1} = h_7 = 1570, k_{l-1} = k_7 = 273,$$

$$\eta = h_{l-1} + k_{l-1}\sqrt{m} = 1520 + 273\sqrt{31}, \quad N(\eta) = (-1)^l = 1.$$

Portanto, a unidade fundamental de $\mathcal{O}_{Q(\sqrt{31})}$ é $1520 + 273\sqrt{31}$.

Exemplo 3.7.16. Para $m = 41$, segue que

$$m = 41 \equiv 1 \pmod{8}.$$

Calculamos os valores do *Passo 2*.

n	P_n	Q_n	y_n	h_n	k_n
-1				1	0
0	0	1	6	6	1
1	6	5	2	13	2
2	4	5	2	32	5
3	6	1	12	397	62
4	6	5	2	826	129

Note que $P_4 = P_1 = 6$ e $Q_4 = Q_1 = 5$. Dessa forma, $N = 4$, $l = N - 1 = 3$, $h_{l-1} = h_2 = 32$ e $k_{l-1} = k_2 = 5$. Assim,

$$\eta = h_{l-1} + k_{l-1}\sqrt{m} = 32 + 5\sqrt{41}, \quad N(\eta) = (-1)^l = (-1)^3 = -1.$$

Portanto, a unidade fundamental de $\mathcal{O}_{Q(\sqrt{41})}$ é $32 + 5\sqrt{41}$ com norma -1 .

Exemplo 3.7.17. Para $m = 82$, segue que

$$m = 82 \equiv 2 \pmod{4}.$$

Assim,

n	P_n	Q_n	y_n	h_n	k_n
-1				1	0
0	0	1	9	9	1
1	9	1	18	163	18
2	9	1	18	2943	325

Como $P_2 = P_1 = 9$ e $Q_2 = Q_1 = 1$, segue que

$$N = 2, l = N - 1 = 1, h_{l-1} = h_0 = 9, k_{l-1} = k_0 = 1,$$

$$\eta = h_{l-1} + k_{l-1}\sqrt{m} = 9 + 1\sqrt{82}, \quad N(\eta) = (-1)^l = -1.$$

Portanto, a unidade fundamental de $\mathcal{O}_{Q(\sqrt{82})}$ é $9 + \sqrt{82}$ de norma -1 .

Note que, até agora, apresentamos um exemplo de cada caso do *Passo 4*. A seguir, apresentamos alguns exemplos do *Passo 5*.

Exemplo 3.7.18. Para $m = 13$, segue que

$$m = 13 \equiv 5 \pmod{8}.$$

Assim,

n	P_n	Q_n	y_n	h_n	k_n
-1				1	0
0	0	1	3	3	1
1	3	4	1	4	1
2	1	3	1	7	2
3	2	3	1	11	3
4	1	4	1	18	5
5	3	1	6	119	33
6	3	4	1	137	38

Como $P_6 = P_1 = 3$ e $Q_6 = Q_1 = 4$, segue que

$$N = 6, l = N - 1 = 5, h_{l-1} = h_4 = 18, k_{l-1} = k_4 = 5.$$

A seguir, encontramos os possíveis valores de A e B . Se A é ímpar, então

$$A|h_{l-1}, \text{ com } 1 \leq A < 2(h_{l-1})^{1/3},$$

e assim, $A | 18$. Como A é ímpar, segue que $A | 9$, com $1 \leq A < 2(\sqrt[3]{18}) \approx 2(2.6207) = 5.2414$, ou seja, $A = 1$ ou $A = 3$. Agora, se B é ímpar, então

$$B|k_{l-1}, \text{ com } 1 \leq B < 2\left(\frac{k_{l-1}}{m}\right)^{1/3},$$

e assim, $B|5$, com $1 \leq B < 2\left(\sqrt[3]{\frac{5}{13}}\right) \approx 2(0.72724) = 1.45448$, ou seja, $B = 1$. Assim, os possíveis pares são $(A, B) = (1, 1)$ ou $(A, B) = (3, 1)$. Mas, apenas o segundo satisfaz o par de equações, uma vez que

$$A^3 + 3AB^2m = 8h_{l-1} = 8.18 = 144 \Rightarrow 3^3 + 3.3.1^2.13 = 27 + 117 = 144$$

$$3A^2B + B^3m = 8k_{l-1} = 8.5 = 40 \Rightarrow 3.3^2.1 + 1^3.13 = 27 + 13 = 40,$$

e que o par $(A, B) = (1, 1)$ não satisfaz as equações acima. Logo, a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{13})}$ é

$$\eta = \frac{3 + \sqrt{13}}{2}, \text{ com } N(\eta) = -1.$$

Exemplo 3.7.19. Para $m = 37$, segue que $37 \equiv 5 \pmod{8}$, e assim,

n	P_n	Q_n	y_n	h_n	k_n
-1				1	0
0	0	1	6	6	1
1	6	1	12	73	12
2	6	1	12	882	145

Logo, $P_2 = P_1 = 6$ e $Q_2 = Q_1 = 1$, e assim,

$$N = 2, l = N - 1 = 1, h_{l-1} = h_0 = 6, k_{l-1} = k_0 = 1.$$

Para esse caso, precisamos encontrar um par de inteiros ímpares (A, B) que satisfaçam as seguintes equações:

$$\begin{cases} A^3 + 3(37)AB^2 = 8h_{l-1} = 8h_0 \Leftrightarrow A^3 + 111AB^2 = 48, \\ 3A^2B + 37B^3 = 8k_{l-1} = 8k_0 \Leftrightarrow 2A^3B + 37B^3 = 8. \end{cases}$$

Entretanto, esse par de equações não possui solução em inteiros positivos. Portanto, a unidade fundamental $\eta > 1$ de $\mathcal{O}_{\mathbb{Q}(\sqrt{37})}$ é

$$\eta = h_{l-1} + k_{l-1}\sqrt{m} = 6 + \sqrt{37}, \text{ com } N(\eta) = -1.$$

4 Teorema das unidades de Dirichlet

Seja $\mathbb{K}$ um corpo de números algébrico de grau $n \geq 2$ sobre $\mathbb{Q}$. Seja $\{\sigma_1, \dots, \sigma_n\}$ o conjunto de todos monomorfismos $\mathbb{K} \rightarrow \mathbb{C}$. Se $\sigma_i(\mathbb{K}) \subseteq \mathbb{R}$, σ_i é chamada uma imersão real; caso contrário, σ_i é chamado uma imersão complexa. Como de costume, $\bar{\alpha}$ denota o conjugado complexo de $\alpha \in \mathbb{C}$. Assim, para todo $\alpha \in \mathbb{K}$, seja

$$\overline{\sigma_i}(\alpha) = \overline{\sigma_i(\alpha)}$$

Como a conjugação complexa é um automorfismo de $\mathbb{C}$, $\overline{\sigma_i}$ é um monomorfismo de $\mathbb{K}$ em $\mathbb{C}$. Consequentemente, $\overline{\sigma_i} = \sigma_j$, para algum j . Ainda, note que $\overline{\sigma_i} = \sigma_i$ se, e somente, se σ_i é real e $\overline{(\overline{\sigma_i})} = \sigma_i$. Dessa forma, vemos que os monomorfismos complexos ocorrem como pares conjugados. Enumeramos os monomorfismos de forma que $\sigma_1, \dots, \sigma_r$ são reais e $\sigma_{r+1}, \dots, \sigma_{r+s}$ são complexos e

$$\sigma_{r+s+1} = \overline{\sigma_{r+1}}, \dots, \sigma_n = \sigma_{r+2s} = \overline{\sigma_{r+s}}.$$

Os corpos conjugados $\mathbb{K}^{(i)}$ de $\mathbb{K}$ são definidos por

$$\mathbb{K}^{(i)} = \sigma_i(\mathbb{K}), \text{ onde } i = 1, 2, \dots, n.$$

Os r corpos conjugados $\mathbb{K}^{(1)}, \dots, \mathbb{K}^{(r)}$ são reais e os $(n - r)$ corpos $\mathbb{K}^{(r+1)}, \dots, \mathbb{K}^{(n)}$ são não reais com

$$\mathbb{K}^{(r+s+1)} = \overline{\mathbb{K}^{(r+1)}}, \dots, \mathbb{K}^{(n)} = \mathbb{K}^{(r+2s)} = \overline{\mathbb{K}^{(r+s)}}.$$

Note ainda que

$$n = r + 2s \tag{4.1}$$

e

$$r + s \geq \frac{1}{2}(r + 2s) = \frac{n}{2} \geq 1.$$

Se $s = 0$, então todos os corpos conjugados de $\mathbb{K}$ são reais e $\mathbb{K}$ é chamado um corpo totalmente real. Se $r = 0$, então $\mathbb{K}$ e todos seus conjugados são não reais e $\mathbb{K}$ é chamado um corpo totalmente complexo ou totalmente imaginário.

Pelo Teorema do Elemento Primitivo (2.2.20), segue que $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo de números de grau n . Sejam $\theta_1 = \theta, \theta_2, \dots, \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Considere que exista exatamente m corpos distintos entre os corpos conjugados $\mathbb{K} = \mathbb{Q}(\theta_1), \mathbb{Q}(\theta_2), \dots, \mathbb{Q}(\theta_n)$, então $m|n$ e cada corpo distinto aparece $\frac{n}{m}$ vezes. Se $m = 1$, então $\mathbb{Q}(\theta_1) = \dots = \mathbb{Q}(\theta_n) = \mathbb{K}$ e o corpo $\mathbb{K}$ é dito uma extensão normal sobre $\mathbb{Q}$, ou seja, se $\mathbb{K}$ é normal, então $\mathbb{K}$ é totalmente real ou totalmente complexo, já que todos os corpos conjugados de $\mathbb{K}$ coincidem.

Outra maneira de definir uma extensão de corpos $\mathbb{K} \subseteq \mathbb{L}$ normal é se todo polinômio irreduzível sobre $\mathbb{K}$ que tem uma raiz em $\mathbb{K}$ se decompõe em $\mathbb{L}$. Assim, se satisfizer essa definição, podemos concluir se o corpo será totalmente real ou complexo.

Exemplo 4.0.1. Considere o polinômio cúbico $p(x) = x^3 - 6x + 2 \in \mathbb{Z}[x]$. Observe que $x^3 - 6x + 2$ é irredutível sobre $\mathbb{Q}$ pelo critério de Eisenstein, uma vez que tomando $p = 2$, segue que $2|2 = a_0$, $2|-6 = a_1$, $2|0 = a_2$, $2 \nmid 1 = a_3$ e $2^2 = 4 \nmid 2 = a_0$. Além disso, o discriminante dessa cúbica é dado por

$$D(p) = -4(a_1)^3 - 27(a_0)^2 = -4(-6)^3 - 27(2)^2 = 864 - 108 = 756 > 0.$$

Dessa forma, é irredutível e tem 3 raízes reais. Portanto, o corpo cúbico $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta^3 - 6\theta + 2 = 0$ é totalmente real.

Exemplo 4.0.2. Considere o corpo $\mathbb{K} = \mathbb{Q}(\sqrt{2} + i)$. Note que $\mathbb{K}$ é totalmente complexo, uma vez que os conjugados de $\theta = \sqrt{2} + 1$ são dados por $\pm\sqrt{2} \pm i$ e estes são todos não reais.

4.1 Valorizações de elementos de um corpo de números

Nessa seção, apresentamos a definição e as propriedades de valorizações que precisamos para provar o Teorema das Unidades de Dirichlet. Daqui em diante, consideramos uma base integral $\{\omega_1, \dots, \omega_n\}$ para $\mathbb{K}$.

Se $a \in \mathcal{O}_{\mathbb{K}}$, então as suas coordenadas são determinadas unicamente por inteiros $c_1, \dots, c_n$ dados por

$$a = c_1\omega_1 + \dots + c_n\omega_n.$$

Considere

$$\mathcal{M} = \max_{1 \leq i, j \leq n} |\sigma_i(\omega_j)| \quad (4.2)$$

e

$$D = \det(\sigma_i(\omega_j)) \quad (4.3)$$

Como $\{\omega_1, \dots, \omega_n\}$ é uma base integral para $\mathbb{K}$, segue que

$$D^2 = d(\mathbb{K}).$$

Logo,

$$|D| = |d(\mathbb{K})|^{(\frac{1}{2})} \quad \text{e} \quad D \neq 0. \quad (4.4)$$

A seguir, apresentamos a definição de valorização e suas propriedades.

Definição 4.1.1. (Valorização de um elemento de um corpo de números) Para $a \in \mathbb{K}$, definimos

$$\beta_i(a) = |\sigma_i(a)|, \quad \text{onde } i = 1, 2, \dots, r + s.$$

Os $r + s$ valores de $\beta_i(a)$, onde $i = 1, 2, \dots, r + s$, são chamados de **valorizações** de a .

Proposição 4.1.2. Se $\beta_i(a) = |\sigma_i(a)|$, onde $i = 1, 2, \dots, r + s$, é a valorização de a , então

$$\beta_i(a) = |\sigma_i(a)| = \sqrt{\sigma_i(a) \cdot \overline{\sigma_i(a)}}$$

é um número algébrico real não negativo de grau no máximo $2n^2$.

Demonstração. Como $\sigma_i(a) \in \mathbb{K}^{(i)}$ e $[\mathbb{K}^{(i)} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}] = n$, segue que $\sigma_i(a)$ é um número algébrico de grau no máximo n . Portanto, $\overline{\sigma_i(a)}$ também é um número algébrico de grau no máximo n . Consequentemente, $\sigma_i(a) \cdot \overline{\sigma_i(a)}$ é um número algébrico de grau no máximo n^2 . Agora,

$$\sigma_i(a) \overline{\sigma_i(a)} = |\sigma_i(a)|^2 \Rightarrow \beta_i(a) = |\sigma_i(a)| = \sqrt{\sigma_i(a) \cdot \overline{\sigma_i(a)}}$$

tem grau no máximo $2n^2$ e é um número algébrico não negativo. $\square$

Exemplo 4.1.3. Seja $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$. Neste caso, $n = 3$, $r = 1$ e $s = 1$. Assim, os três monomorfismos $\mathbb{K} \rightarrow \mathbb{C}$ são dados por

$$\begin{aligned}\sigma_1(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \\ \sigma_2(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + \omega b\sqrt[3]{2} + \omega^2 c(\sqrt[3]{2})^2 \\ \sigma_3(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + \omega^2 b\sqrt[3]{2} + \omega c(\sqrt[3]{2})^2,\end{aligned}$$

onde $\omega = e^{\frac{2\pi i}{3}} = \frac{-1 + i\sqrt{3}}{2}$ é uma raiz cúbica complexa da unidade. Note que $\sigma_3 = \overline{\sigma_2}$. Assim,

$$\beta_1(\sqrt[3]{2} + (\sqrt[3]{2})^2) = |\sigma_1(\sqrt[3]{2} + (\sqrt[3]{2})^2)| = |\sqrt[3]{2} + (\sqrt[3]{2})^2| = \sqrt[3]{2} + (\sqrt[3]{2})^2$$

e

$$\begin{aligned}\beta_2(\sqrt[3]{2} + (\sqrt[3]{2})^2) &= |\sigma_2(\sqrt[3]{2} + (\sqrt[3]{2})^2)| = |\omega\sqrt[3]{2} + \omega^2(\sqrt[3]{2})^2| \\ &= \left| \left(\frac{-1 + i\sqrt{3}}{2} \right) \sqrt[3]{2} + \left(\frac{-1 - i\sqrt{3}}{2} \right) (\sqrt[3]{2})^2 \right| \\ &= \left| \frac{-\sqrt[3]{2}}{2} + \frac{i\sqrt{3}\sqrt[3]{2}}{2} - \frac{(\sqrt[3]{2})^2}{2} - \frac{i\sqrt{3}(\sqrt[3]{2})^2}{2} \right| \\ &= \left| \frac{-1}{2}(\sqrt[3]{2} + (\sqrt[3]{2})^2) + \frac{1\sqrt{3}}{2}(\sqrt[3]{2} - (\sqrt[3]{2})^2) \right| \\ &= \sqrt{\frac{(\sqrt[3]{2} + (\sqrt[3]{2})^2)^2 + 3(\sqrt[3]{2} - (\sqrt[3]{2})^2)^2}{4}} \\ &= \sqrt{\frac{[(\sqrt[3]{2})^2 + 2(\sqrt[3]{2})(\sqrt[3]{2})^2 + ((\sqrt[3]{2})^2)^2] + 3[(\sqrt[3]{2})^2 - 2(\sqrt[3]{2})(\sqrt[3]{2})^2 + ((\sqrt[3]{2})^2)^2]}{4}} \\ &= \sqrt{\frac{(\sqrt[3]{2})^2 + 2.2 + 2\sqrt[3]{2} + 3(\sqrt[3]{2})^2 - 3.2.2 + 2\sqrt[3]{2}}{4}} \\ &= \sqrt{\frac{-8 + 4(2\sqrt[3]{2}) + 4(\sqrt[3]{2})^2}{4}} = \sqrt{-2 + 2\sqrt[3]{2} + (\sqrt[3]{2})^2}.\end{aligned}$$

Proposição 4.1.4. Se $m \in \mathbb{Z}$, então

$$\beta_i(m) = |m|, \quad \text{onde } i = 1, \dots, r + s.$$

Demonstração. Observe que, para $i = 1, \dots, r+s$, cada $\sigma_i : \mathbb{K} \longrightarrow \mathbb{C}$ é um monomorfismo tal que

$$\sigma_i(a) = a, \quad \text{para todo } a \in \mathbb{Q}.$$

Como $m \in \mathbb{Z} \subseteq \mathbb{Q}$, segue que

$$\beta_i(m) = |\sigma_i(m)| = |m|, \quad \text{onde } i = 1, \dots, r+s,$$

o que prova a proposição. $\square$

Proposição 4.1.5. *Se $a, b \in \mathbb{K}$, então*

$$\beta_i(a) \cdot \beta_i(b) = \beta_i(ab), \quad \text{onde } i = 1, \dots, r+s.$$

Demonstração. Se $a, b \in \mathbb{K}$, então $ab \in \mathbb{K}$. Assim, para $i = 1, \dots, r+s$, segue que

$$\beta_i(ab) = |\sigma_i(ab)|$$

Como σ_i é um monomorfismo, segue que

$$|\sigma_i(ab)| = |\sigma_i(a) \cdot \sigma_i(b)| = |\sigma_i(a)| \cdot |\sigma_i(b)|.$$

Portanto,

$$\beta_i(a) \cdot \beta_i(b) = \beta_i(ab), \quad \text{onde } i = 1, \dots, r+s,$$

o que prova a proposição. $\square$

A seguir, veremos que os inteiros de $\mathbb{K}$ com coordenadas limitadas têm valorizações limitadas.

Proposição 4.1.6. *Se $a \in \mathcal{O}_{\mathbb{K}}$ tal que suas coordenadas c_i ($i = 1, \dots, n$) satisfazem $|c_i| \leq C$, então*

$$\beta_i(a) \leq n \cdot c \cdot \mathcal{M}, \quad \text{onde } i = 1, \dots, n.$$

Demonstração. Lembre que $\{\omega_1, \dots, \omega_n\}$ é uma base integral de $\mathbb{K}$. Daí, para $a \in \mathcal{O}_{\mathbb{K}}$,

$$a = c_1\omega_1 + \dots + c_n\omega_n \Rightarrow \sigma_i(a) = c_1\sigma_i(\omega_1) + \dots + c_n\sigma_i(\omega_n), \quad \text{onde } i = 1, \dots, n.$$

Portanto, para $i = 1, \dots, r+s$, segue que

$$\beta_i(a) = |\sigma_i(a)| = |c_1\sigma_i(\omega_1) + \dots + c_n\sigma_i(\omega_n)| \leq |c_1| \cdot |\sigma_i(\omega_1)| + \dots + |c_n| \cdot |\sigma_i(\omega_n)|$$

Como $|c_i| \leq C$ por hipótese e $\mathcal{M} = \max |\sigma_i(\omega_j)|$ por (4.2), segue que

$$|c_1| \cdot |\sigma_i(\omega_1)| + \dots + |c_n| \cdot |\sigma_i(\omega_n)| \leq C\mathcal{M} + \dots + C\mathcal{M} = nC\mathcal{M}.$$

Portanto, $\beta_i(a) \leq nC\mathcal{M}$. $\square$

Proposição 4.1.7. *Se $a \in \mathcal{O}_{\mathbb{K}}$ é tal que*

$$\beta_i(a) \leq L, \quad \text{onde } i = 1, \dots, r+s,$$

então as coordenadas c_i , onde $i = 1, \dots, n$, de a , satisfazem

$$|c_i| \leq \frac{n!L\mathcal{M}^{n-1}}{|d(\mathbb{K})|^{\frac{1}{2}}}, \quad \text{para } i = 1, \dots, n.$$

Demonstração. Lembre que

$$a = c_1\omega_1 + \dots + c_n\omega_n,$$

onde c_i são as coordenadas de a , para $i = 1, \dots, n$, e $\{\omega_1, \dots, \omega_n\}$ é uma base integral de $\mathbb{K}$. Assim,

$$\sigma_i(a) = c_1\sigma_i(\omega_1) + \dots + c_n\sigma_i(\omega_n), \quad \text{para } i = 1, \dots, n.$$

Pela regra de Cramer, segue que

$$c_i = \frac{N_i}{D}, \quad \text{para } i = 1, \dots, n, \quad (4.5)$$

onde o determinante é definido na Equação (4.3), isto é,

$$D = \det(\sigma_i(\omega_j)), \quad \text{para } 1 \leq i, j \leq n.$$

O determinante N_j é formado por D trocando a i -ésima coluna por $[\sigma_1(a)\sigma_2(a)\dots\sigma_n(a)]$. Expandindo N_i pela sua i -ésima coluna, segue que

$$N_i = \sum_{k=1}^n \sigma_k(a)(-1)^{k+1} \Delta_k,$$

onde cada Δ_k é determinante de uma matriz $(n-1) \times (n-1)$ cujas entradas pertencem a $\{\sigma_p(\omega_q) \mid p, q = 1, \dots, n\}$. Lembre que

$$\mathcal{M} = \max_{1 \leq p, q \leq n} |\sigma_p(\omega_q)| \Rightarrow |\sigma_p(\omega_q)| \leq \mathcal{M}, \quad \text{para todo } p, q \in \{1, \dots, n\}.$$

$$|\Delta_k| \leq (n-1)!\mathcal{M}^{n-1}, \quad \text{para } i = 1, \dots, n.$$

Agora,

$$\begin{aligned} |N_i| &= \left| \sum \sigma_k(a)(-1)^{k+1} \Delta_k \right| = \left| \sum \sigma_k(a)(-1)^{k+1} \right| \cdot |\Delta_k| \\ &\leq \left| \sum_{k=1}^n \beta_i(a) \right| (n-1)!\mathcal{M}^{(n-1)} = \sum_{k=1}^n \beta_i(a)(n-1)!\mathcal{M}^{(n-1)} \\ &\leq nL(n-1)!\mathcal{M}^{(n-1)} = n!L\mathcal{M}^{(n-1)}. \end{aligned}$$

Dessa forma,

$$|N_i| \leq n!L\mathcal{M}^{(n-1)}. \quad (4.6)$$

Por fim,

$$c_i \stackrel{(4.5)}{=} \frac{N_i}{D} \stackrel{(4.6)}{=} \frac{N_i}{|d(\mathbb{K})|^{\frac{1}{2}}} \stackrel{(4.4)}{\leq} \frac{n!L\mathcal{M}}{|d(\mathbb{K})|^{\frac{1}{2}}}, \quad \text{para } i = 1, \dots, n,$$

o que prova a proposição. $\square$

Observe que a Proposição 4.1.7 fornece uma recíproca da Proposição 4.1.6, isto é, os inteiros de $\mathbb{K}$ com valorizações limitadas têm coordenadas limitadas. O resultado a seguir é uma consequência imediata deste fato.

Corolário 4.1.8. *Existem apenas uma quantidade finita de $a \in \mathcal{O}_{\mathbb{K}}$ cujas valorizações $\beta_i(a)$, onde $i = 1, \dots, r + s$, são menores do que um determinado limite.*

Demonstração. Considere $a \in \mathcal{O}_{\mathbb{K}}$ tal que

$$\beta_i(a) \leq L, \quad \text{onde } i = 1, \dots, r+s.$$

Pela Proposição 4.1.7, para

$$a = c_1\omega_1 + \dots + c_n\omega_n, \text{ onde } c_i \in \mathbb{Z},$$

segue que

$$|c_i| \leq \left\lfloor \frac{n!L\mathcal{M}}{|d(\mathbb{K})|^{\frac{1}{2}}} \right\rfloor \Rightarrow - \left\lfloor \frac{n!L\mathcal{M}}{|d(\mathbb{K})|^{\frac{1}{2}}} \right\rfloor \leq c_i \leq \left\lfloor \frac{n!L\mathcal{M}}{|d(\mathbb{K})|^{\frac{1}{2}}} \right\rfloor.$$

Assim, o número de possibilidades para cada c_i é

$$2 \cdot \left\lfloor \frac{n!L\mathcal{M}}{|d(\mathbb{K})|^{\frac{1}{2}}} \right\rfloor + 1,$$

onde soma-se 1 para considerar a possibilidade de igualdade. Assim, o número de $a \in \mathcal{O}_{\mathbb{K}}$ com $\beta_i(a) \leq L$, onde $i = 1, \dots, r+s$, é no máximo

$$\left(2 \cdot \left\lfloor \frac{n!L\mathcal{M}}{|d(\mathbb{K})|^{\frac{1}{2}}} \right\rfloor + 1 \right)^n,$$

que é um número finito. Portanto, a quantidade de $a \in \mathcal{O}_{\mathbb{K}}$ tal que $\beta_i(a) \leq L$, onde $i = 1, \dots, r+s$, é finita. $\square$

Proposição 4.1.9. *Se $a \in \mathbb{K}$, então*

$$N(\langle a \rangle) = \prod_{i=1}^{r+s} \beta_i(a)^{d_i},$$

onde

$$d_i = \begin{cases} 1, & \text{se } i = 1, \dots, r; \\ 2, & \text{se } i = r+1, \dots, r+s. \end{cases} \quad (4.7)$$

Demonstração. Aplicando a norma, segue que

$$\begin{aligned} N(\langle a \rangle) &= |N(a)| = \left| \prod_{i=1}^n \sigma_i(a) \right| = \left| \prod_{i=1}^{r+s} \sigma_i(a) \prod_{i=r+s+1}^{r+2s} \sigma_i(a) \right| = \left| \prod_{i=1}^{r+s} \sigma_i(a) \prod_{i=r+1}^{r+s} \sigma_{i+s}(a) \right| \\ &= \left| \prod_{i=1}^{r+s} \sigma_i(a) \prod_{i=r+1}^{r+s} \overline{\sigma_i(a)} \right| = \left| \prod_{i=1}^{r+s} \sigma_i(a) \prod_{i=r+1}^{r+s} \overline{\sigma_i(a)} \right| = \left| \prod_{i=1}^r \sigma_i(a) \prod_{i=r+1}^{r+s} \sigma_i(a) \cdot \overline{\sigma_i(a)} \right| \\ &= \left| \prod_{i=1}^r \sigma_i(a) \prod_{i=r+1}^{r+s} |\sigma_i(a)|^2 \right| = \prod_{i=1}^r \underbrace{|\sigma_i(a)|}_{\beta_i(a)} \prod_{i=r+1}^{r+s} \underbrace{|\sigma_i(a)|^2}_{(\beta_i(a))^2} = \prod_{i=1}^{r+s} (\beta_i(a))^{d_i}, \end{aligned}$$

onde d_i é definido na Equação (4.7). $\square$

Corolário 4.1.10. *Se ϵ é uma unidade de $\mathcal{O}_{\mathbb{K}}$, então*

$$\prod_{i=1}^{r+s} (\beta_i(\epsilon))^{d_i} = 1, \quad d_i = \begin{cases} 1, & \text{se } i = 1, \dots, r; \\ 2, & \text{se } i = r+1, \dots, r+s. \end{cases}$$

Demonstração. Note que $N(\langle \epsilon \rangle) = N(\langle 1 \rangle) = 1$, uma vez que ϵ é uma unidade de $\mathcal{O}_{\mathbb{K}}$. Logo, pela Proposição 4.1.9, segue que

$$\prod_{i=1}^{r+s} (\beta_i(\epsilon))^{d_i} = N(\langle \epsilon \rangle) = N(\langle 1 \rangle) = 1,$$

o que prova o corolário. $\square$

Proposição 4.1.11. *Se p_i e q_i , onde $i = 1, \dots, r+s$, são números racionais tais que*

$$0 \leq p_i < q_i, \quad \text{onde } i = 1, \dots, r+s,$$

então existe $a \in \mathbb{K}$ tal que

$$p_i < \beta_i(a) < q_i, \quad \text{onde } i = 1, \dots, r+s.$$

Demonstração. Seja $h_i = \frac{1}{2}(p_i + q_i) \in \mathbb{Q}$ tal que $p_i < h_i < q_i$, para $i = 1, \dots, r+s$. Para $i = r+s+1, \dots, r+2s$, considere $h_i = h_{i-s}$. Portanto, h_i está definido para $i = 1, \dots, n$ e $h_{r+s+j} = h_{r+j}$ para $j = 1, \dots, s$. Agora, considere o sistema linear com n equações e n incógnitas $b_1, b_2, \dots, b_n$ dado por

$$\begin{cases} b_1\sigma_1(\omega_1) + b_2\sigma_1(\omega_2) + \dots + b_n\sigma_1(\omega_n) = h_1 \\ b_1\sigma_2(\omega_1) + b_2\sigma_2(\omega_2) + \dots + b_n\sigma_2(\omega_n) = h_2 \\ \vdots \\ b_1\sigma_n(\omega_1) + b_2\sigma_n(\omega_2) + \dots + b_n\sigma_n(\omega_n) = h_n \end{cases}$$

Assim,

$$b_1\sigma_i(\omega_1) + b_2\sigma_i(\omega_2) + \dots + b_n\sigma_i(\omega_n) = h_i, \quad \text{para } i = 1, \dots, n. \quad (4.8)$$

Note que todos os termos constantes desse sistema são reais. Além disso, o determinante da matriz dos coeficientes desse sistema é

$$D = \det(\sigma_i(\omega_j)) \neq 0. \quad (4.9)$$

Dessa forma, o sistema tem uma solução única $(b_1, \dots, b_n) \in \mathbb{C}^n$. As primeiras r equações do Sistema (4.8) tem coeficientes reais, uma vez que σ_i , onde $i = 1, \dots, r$, são monomorfismos reais. Já as restantes $n-2 = 2s$ equações possuem coeficientes em pares conjugados complexos, ou seja, as partes complexas irão se cancelar. Portanto, $(b_1, \dots, b_n) \in \mathbb{R}^n$. Agora, se

$$\delta = \min_{1 \leq i \leq r+s} \frac{(q_i - p_i)}{2\mathcal{M}_n},$$

então

$$0 < \delta < \frac{(q_i - p_i)}{2\mathcal{M}_n}, \quad \text{onde } i = 1, \dots, r+s. \quad (4.10)$$

Em seguida, escolha $c_i \in \mathbb{Q}$ tal que

$$|b_i - c_i| < \delta, \quad \text{onde } i = 1, \dots, n.$$

Tomando

$$a = c_1\omega_1 + \dots + c_n\omega_n \in \mathbb{K},$$

para $i = 1, \dots, n$, segue que

$$\sigma_i(a) = c_1\sigma_i(\omega_1) + \dots + c_n\sigma_i(\omega_n),$$

e assim,

$$\sigma_i(a) - h_i = (c_1\sigma_i(\omega_1) + \dots + c_n\sigma_i(\omega_n)) - (b_1\sigma_i(\omega_1) + b_2\sigma_i(\omega_2) \dots + b_n\sigma_i(\omega_n)),$$

e portanto,

$$\sigma_i(a) - h_i = (c_1 - b_1)(\sigma_i(\omega_1)) + \dots + (c_n - b_n)(\sigma_i(\omega_n)).$$

Logo, para $i = 1, \dots, r + s$, segue que

$$\begin{aligned} |\sigma_i(a) - h_i| &\leq |c_1 - b_1| \cdot |\sigma_i(\omega_1)| + \dots + |c_n - b_n| \cdot |\sigma_i(\omega_n)| \\ &\leq |c_1 - b_1| \mathcal{M} + \dots + |c_n - b_n| \mathcal{M} = \mathcal{M} \underbrace{(|c_1 - b_1| + \dots + |c_n - b_n|)}_{n \text{ termos}} \\ &< \mathcal{M}n\delta \leq \mathcal{M}n \left(\frac{q_i - p_i}{2\mathcal{M}n} \right) = \frac{q_i - p_i}{2}, \end{aligned}$$

e assim,

$$|\sigma_i(a) - h_i| < \frac{q_i - p_i}{2}.$$

Agora, pela desigualdade triangular, segue que

$$||\sigma_i(a)| - |h_i|| \leq |\sigma_i(a) - h_i|.$$

Dessa forma,

$$\begin{aligned} ||\sigma_i(a)| - |h_i|| &\leq |\sigma_i(a) - h_i| < \frac{q_i - p_i}{2} \\ \Rightarrow ||\sigma_i(a)| - |h_i|| &< \frac{q_i - p_i}{2} \\ \Rightarrow -\left(\frac{q_i - p_i}{2}\right) &< |\sigma_i(a)| - |h_i| < \left(\frac{q_i - p_i}{2}\right) \\ \Rightarrow -\left(\frac{q_i - p_i}{2}\right) + |h_i| &< |\sigma_i(a)| < \left(\frac{q_i - p_i}{2}\right) + |h_i|. \end{aligned}$$

Como, por hipótese $0 \leq p_i < q_i$, segue que $h_i = \frac{p_i + q_i}{2} \geq 0$. Assim,

$$\begin{aligned} -\left(\frac{q_i - p_i}{2}\right) + |h_i| &< \underbrace{|\sigma_i(a)|}_{\beta_i(a)} < \left(\frac{q_i - p_i}{2}\right) + |h_i| \\ \Rightarrow -\left(\frac{q_i - p_i}{2}\right) + h_i &< \beta_i(a) < \left(\frac{q_i - p_i}{2}\right) + h_i \\ \Rightarrow -\frac{q_i - p_i}{2} + \frac{p_i + q_i}{2} &< \beta_i(a) < \frac{q_i - p_i}{2} + \frac{p_i + q_i}{2} \\ \Rightarrow p_i &< \beta_i(a) < q_i. \end{aligned}$$

Portanto, mostramos que existe $a \in \mathbb{K}$ tal que $p_i < \beta_i(a) < q_i$, onde $i = 1, \dots, r + s$. $\square$

Definição 4.1.12. Seja A um domínio e $\mathbb{L}$ seu corpo de frações. Um A -submódulo I de $\mathbb{L}$ é chamado **ideal fracionário** de A se existe um $d \in A - \{0\}$ tal que $dI \subset A$. Quando $d = 1$, o ideal I é chamado **ideal inteiro**.

Proposição 4.1.13. *Seja k um inteiro positivo. Se $I \neq 0$ é um ideal de $\mathcal{O}_{\mathbb{K}}$ (inteiro ou fracionário) tal que $N(I) \leq k^n$, então I contém um elemento $a \neq 0$ com $\beta_i(a) \leq n\mathcal{M}k$ ($i = 1, \dots, r + s$).*

Demonstração. Primeiro vamos considerar o caso que I é ideal inteiro. Seja

$$S = \{b \in \mathcal{O}_{\mathbb{K}} \mid b = b_1\omega_1 + \dots + b_n\omega_n; \ b_1, \dots, b_n \in \underbrace{\{0, 1, \dots, k\}}_{k+1 \text{ elementos}}\}.$$

A quantidade de elementos de S é

$$(k+1)^n > k^n \stackrel{\text{hipótese}}{\geq} N(I).$$

Dessa forma, existem $b', b'' \in S$, com $b' \neq b''$ tais que

$$\underbrace{b' \equiv b'' \pmod{I}}_{I \mid b' - b''}.$$

Seja $a = b' - b'' \neq 0$. Assim, $a \in \mathcal{O}_{\mathbb{K}}$ e $a \equiv 0 \pmod{I}$, isto é, $a \in I$. Além disso, as coordenadas $a_1, \dots, a_n$ de a satisfazem

$$|a_i| = |b'_i - b''_i| \leq k, \quad \text{onde } i = 1, \dots, n,$$

onde os b'_i são as coordenadas de b' e os b''_i são de b'' , onde $i = 1, \dots, n$. Assim, pela Proposição 4.1.6, segue que

$$\beta_i(a) \leq nk\mathcal{M}, \quad \text{onde } i = 1, \dots, r + s.$$

Portanto, finalizamos o caso em que I é um ideal inteiro. Vamos agora fazer o caso em que I é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$ satisfazendo $N(I) \leq k^n$. Considere y um denominador comum de I . Sejam $y = y_1, y_2, \dots, y_n$ os conjugados de y tais que $N(y) = y_1 \dots y_n \in \mathbb{Z} - \{0\}$ e $N(y).I = y_1 \dots y_n.(yI)$ é um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$. Se $m = |N(y)|$, então m é um inteiro positivo tal que $J = mI$ é um ideal inteiro de $\mathcal{O}_{\mathbb{K}}$ com

$$N(J) = N(mI) = m^n.N(I) \leq m^n.k^n = (mk)^n.$$

Pelo caso anterior, segue que existe $b \in J$, com $b \neq 0$ tal que

$$\beta_i(b) \leq (mk)n\mathcal{M}, \quad \text{onde } i = 1, \dots, r + s.$$

Como $b \in J$, então existe $a \in I$ tal que $b = ma$. Assim, $a \neq 0$ e pelas Proposições 4.1.4 e 4.1.5, segue que

$$\beta_i(a) = \beta_i\left(\frac{b}{m}\right) = \frac{\beta_i(b)}{\beta_i(m)} \leq \frac{(mk)n\mathcal{M}}{m} = kn\mathcal{M}, \quad \text{onde } i = 1, \dots, r + s.$$

Portanto, finalizamos o caso em que I é ideal fracionário. □

Proposição 4.1.14. *Existe um limite fixo $B > 0$ tal que para cada $a \in \mathbb{K}$ com $\frac{1}{2} < N(\langle a \rangle) \leq 1$, tem-se uma unidade $\epsilon \in \mathcal{O}_{\mathbb{K}}$ tal que*

$$B_j \leq B, \quad \text{onde } j = 1, \dots, r + s.$$

Demonstração. Seja $a \in \mathbb{K}$ tal que $\frac{1}{2} < N(a)$. Seja $I = \langle a \rangle$ de modo que

$$\frac{1}{2} < \underbrace{N(I)}_{N(\langle a \rangle)} \leq 1.$$

Agora, considere S o conjunto de todos os ideais principais I distintos. Pela Proposição 4.1.13, para cada $I = \langle a \rangle$ em S , existe b não nulo tal que

$$\beta_i(b) \leq n\mathcal{M}, \quad \text{onde } i = 1, \dots, r+s.$$

Como $b \in \langle a \rangle$, segue que b pode ser escrito como $b = qa$, para algum $q \neq 0$ de $\mathcal{O}_{\mathbb{K}}$. Dessa forma,

$$\begin{aligned} \frac{N(\langle q \rangle)}{2} &< N(\langle q \rangle).N(I) = N(\langle q \rangle).N(\langle a \rangle) = N(\langle q \rangle \langle a \rangle) = N(\langle qa \rangle) = N(\langle b \rangle) \\ &= \prod_{i=1}^{r+s} (\beta_i(b))^{d_i} \leq \prod_{i=1}^{r+s} (n\mathcal{M})^{d_i} = (n\mathcal{M})^n \Rightarrow N(\langle q \rangle) < 2(n\mathcal{M})^n. \end{aligned}$$

Portanto, existe apenas uma quantidade finita entre os ideais principais $\langle q \rangle$ distintos. Digamos $\langle q_1 \rangle, \dots, \langle q_t \rangle$. Assim, cada $q = \epsilon.q_j$ para alguma unidade ϵ de $\mathcal{O}_{\mathbb{K}}$ e algum $j \in \{1, 2, \dots, t\}$. Seja

$$l = \max_{\substack{i=1, \dots, r+s \\ j=1, \dots, t}} \beta_i(q_j^{-1}).$$

Agora, para cada $i = 1, \dots, r+s$ e $j = 1, \dots, t$, segue que

$$1 = \beta_i(1) = \beta_i(q_j.q_j^{-1}) = \beta_i(q_j)\beta_i(q_j^{-1}) \leq l.\beta_i(q_j).$$

Portanto,

$$\beta_i(\epsilon a) \leq l.\beta_i(q_j)\beta_i(\epsilon a) = l\beta_i(q_j\epsilon a) = l\beta_i(b) \leq l.n.\mathcal{M},$$

ou seja, $\beta_i(\epsilon a) < B$, onde $i = 1, \dots, r+s$ e $B = ln\mathcal{M}$. □

Proposição 4.1.15. *Se $j \in \{1, \dots, r+s-1\}$, então existe $a \in \mathbb{K}$ com $\frac{1}{2} < N(\langle a \rangle) \leq 1$ tal que*

$$\beta_i(a) > B, \quad \text{onde } i = 1, \dots, r+s, \quad \text{com } i \neq j.$$

Demonstração. Se $r+s = 1$, não há nada para mostrar. Dessa forma, suponha que $r+s \geq 2$. Pela Proposição 4.1.11, para $B \in \mathbb{Q}$, onde $i = 1, \dots, r+s$, tal que $0 \leq B < 2^{\frac{1}{n}}B$, $n > 0$, segue que existe $a \in \mathbb{K}$ tal que

$$B < \beta_i(a) < 2^{\frac{1}{n}}B, \quad n > 0, \quad \text{onde } i = 1, \dots, r+s.$$

Ainda, pelo mesmo resultado, segue que

$$\frac{1}{2B^{n-1}} < B_j(a) < \frac{1}{2^{1-\frac{1}{n}}}B^{n-1}, \quad \text{onde } j = 1, \dots, r.$$

e

$$\frac{1}{2^{\frac{1}{2}}B^{\frac{n-2}{2}}} < B_j(a) < \frac{1}{2^{\frac{1}{2}-\frac{1}{n}}}B^{\frac{n-2}{2}}, \quad \text{onde } j = r+1, \dots, r+s-1.$$

Assim,

$$B_i(a) > B, \quad \text{onde } i = 1, \dots, r+s, \quad \text{com } i \neq j.$$

1. Se $j \in \{1, \dots, r\}$, então

$$\begin{aligned} \text{(a)} \quad & (\beta_1(a) \dots \beta_r(a) \beta_{r+1}(a)^2 \dots \beta_{r+s}(a)^2) > B^{r-1} \cdot \frac{1}{2B^{n-1}} (B^2)^s = \frac{B^{(r+2s)-1}}{2B^{n-1}} = \\ & \frac{B^{n-1}}{2B^{n-1}} = \frac{1}{2} \Rightarrow \prod_{i=1}^{r+s} \beta_i(a)^{d_i} > \frac{1}{2}. \\ \text{(b)} \quad & (\beta_1(a) \dots \beta_r(a) \beta_{r+1}(a)^2 \dots \beta_{r+s}(a)^2) < (2^{\frac{1}{n}} B)^{r-1} \cdot \frac{1}{2^{1-\frac{1}{n}} B^{n-1}} (2^{\frac{1}{2}} B)^{2s} = \\ & \frac{2^{\frac{(r+2s)-1}{n}} B^{r+2s-1}}{2^{1-\frac{1}{n}} B^{n-1}} = \frac{2^{\frac{n-1}{n}} B^{n-1}}{2^{\frac{n-1}{n}} B^{n-1}} = 1 \Rightarrow \prod_{i=1}^{r+s} \beta_i(a)^{d_i} < 1. \end{aligned}$$

Pela Proposição 4.1.9, segue que

$$N(\langle a \rangle) = \prod_i^{r+s} \beta_i(a)^{d_i},$$

onde

$$d_i = \begin{cases} 1, & \text{se } i = 1, \dots, r; \\ 2, & \text{se } i = r+1, \dots, r+s. \end{cases}$$

Assim,

$$\frac{1}{2} < N(\langle a \rangle) < 1.$$

2. Se $j = r+1, \dots, r+s-1$, então

$$\begin{aligned} \text{(a)} \quad & (\beta_1(a) \dots \beta_r(a) \beta_{r+1}(a)^2 \dots \beta_{r+s}(a)^2) > B^r (B^2)^{s-1} \left(\frac{1}{2^{\frac{1}{2}} B^{\frac{n-2}{2}}} \right)^2 = \frac{B^{r+2s-2}}{2B^{n-2}} = \\ & \frac{B^{n-2}}{2B^{n-2}} = \frac{1}{2} \Rightarrow \prod_i^{r+s} \beta_i(a)^{d_i} > \frac{1}{2}. \\ \text{(b)} \quad & (\beta_1(a) \dots \beta_r(a) \beta_{r+1}(a)^2 \dots \beta_{r+s}(a)^2) < (2^{\frac{1}{n}} B)^r (2^{\frac{2}{n}} B^2)^{s-1} \left(\frac{1}{2^{\frac{1}{2}-\frac{1}{n}} B^{\frac{n-2}{2}}} \right)^2 = \\ & \frac{2^{\frac{r+2s-2}{n}} B^{r+2s-2}}{2^{1-\frac{2}{n}} B^{n-2}} = 1 \Rightarrow \prod_i^{r+s} \beta_i(a)^{d_i} < 1. \end{aligned}$$

Novamente, pela Proposição 4.1.9, segue que

$$\frac{1}{2} < N(\langle a \rangle) < 1.$$

Portanto, para $j = 1, \dots, r+s-1$, segue que existe $a \in \mathbb{K}$ com

$$\frac{1}{2} < N(\langle a \rangle) < 1$$

tal que

$$\beta_i(a) > B, \quad \text{onde } i = 1, \dots, r+s, \quad \text{com } i \neq j,$$

o que prova o resultado. $\square$

Proposição 4.1.16. *Se $j \in \{1, \dots, r+s-1\}$, então existe uma unidade $\epsilon_j \in \mathcal{O}_{\mathbb{K}}$ tal que*

$$\beta_i(\epsilon_j) < 1, \quad \text{onde } i = 1, 2, \dots, r+s \quad \text{com } i \neq j \quad \text{e} \quad \beta_j(\epsilon_j) > 1.$$

Demonstração. Se $r+s = 1$ não há nada para provar. Dessa forma, suponha que $r+s \geq 2$. Pela Proposição 4.1.15, para cada $j = 1, \dots, r+s-1$, segue que existe $a \in \mathbb{K}$ com $\frac{1}{2} < N(\langle a \rangle) < 1$ tal que

$$\beta_i(a) > B, \quad \text{onde } i = 1, \dots, r+s, \quad \text{com } i \neq j \Rightarrow \frac{1}{\beta_i(a)} < \frac{1}{B}.$$

Mas, pela Proposição 4.1.14, segue que existe uma unidade $\epsilon_j \in \mathcal{O}_{\mathbb{K}}$ tal que

$$\beta_i(\epsilon_j a) \leq B, \quad \text{onde } i = 1, \dots, r+s.$$

Assim, pela Proposição 4.1.5, segue que

$$\beta_i(\epsilon_j) = \beta_i\left(\frac{\epsilon_j a}{a}\right) = \beta_i(\epsilon_j a) \cdot \frac{1}{\beta_i(a)} < B \cdot \frac{1}{B} = 1,$$

e assim,

$$\beta_i(\epsilon_j) < 1, \quad \text{onde } i = 1, \dots, r+s, \quad \text{com } i \neq j.$$

Por fim, como ϵ_j é uma unidade $\mathcal{O}_{\mathbb{K}}$, pelo Corolário 4.1.10, segue que

$$1 = \prod_{i=1}^{r+s} \beta_i(\epsilon_j)^{d_i}.$$

Mas, o produto é 1 e para todo $i \neq j$, $\beta_i(\epsilon_j) > 1$, para $i = j$, $\beta_j(\epsilon_j) > 1$. Logo,

$$\beta_i(\epsilon_j)^{d_i} < (\beta_j(\epsilon_j))^{d_j} \Rightarrow \beta_j(\epsilon_j) > 1,$$

o que prova a proposição. $\square$

Definição 4.1.17. (Unidades Independentes) Seja $\mathbb{K}$ um corpo de números algébrico. Sejam $\epsilon_1, \dots, \epsilon_k$, onde $k \geq 1$, unidades de $\mathcal{O}_{\mathbb{K}}$. As unidades $\epsilon_1, \dots, \epsilon_k$ são ditas **independentes** se, e somente se,

$$\epsilon_1^{r_1} \dots \epsilon_k^{r_k} = 1 \Rightarrow r_1 = \dots = r_k = 0, \quad (r_i \in \mathbb{Z}, \quad \text{onde } i = 1, \dots, k).$$

No próximo resultado, mostramos que as unidades $\epsilon_1, \dots, \epsilon_{r+s-1}$ construídas na Proposição 4.1.16 são independentes.

Teorema 4.1.18. *As unidades $\epsilon_1, \dots, \epsilon_{r+s-1}$ que satisfazem a Proposição 4.1.16 são independentes.*

Demonstração. Se $r+s = 1$ não há o que mostrar. Assim, suponha que $r+s \geq 2$ e que existem inteiros $\rho_1, \dots, \rho_{r+s-1}$, não todos nulos, tais que

$$\prod_{j=1}^{r+s-1} \epsilon_j^{\rho_j} = 1. \tag{4.11}$$

Além disso,

$$\prod_{j=1}^{r+s-1} \epsilon_j^{-\rho_j} = 1,$$

e assim, podemos substituir $(\rho_1, \dots, \rho_{r+s-1})$ por $(-\rho_1, \dots, -\rho_{r+s-1})$, se necessário, para garantir que ao menos um dos $\rho_1, \dots, \rho_{r+s-1}$ é positivo. Se necessário, renomeie cada

unidade $\epsilon_1, \dots, \epsilon_{r+s-1}$ de modo que $\rho_1, \dots, \rho_k$, ($k \geq 1$) sejam positivos e $\rho_{k+1}, \dots, \rho_{r+s-1}$ sejam negativos. A partir das valorizações $\beta_1, \dots, \beta_k$ formamos o produto

$$\beta = \beta_1^{d_1} \dots \beta_k^{d_k},$$

e das restantes valorizações $\beta_{k+1}, \dots, \beta_{r+s}$, formamos

$$\beta' = \beta_{k+1}^{d_{k+1}} \dots \beta_{r+s}^{d_{r+s}}.$$

Pelas Proposições 4.1.4 e 4.1.5, para todo $a, b \in \mathbb{K}$, segue que

$$\begin{cases} \beta(1) = 1 \\ \beta(a)\beta(b) = \beta(ab) \\ \beta'(a)\beta'(b) = \beta'(ab). \end{cases} \quad (4.12)$$

Pelo Corolário 4.1.10, segue que

$$\beta(\epsilon)\beta'(\epsilon) = 1,$$

uma vez que

$$1 = \prod_{i=1}^{r+s} \beta_i(\epsilon)^{d_i} = \prod_{i=1}^k \beta_i(\epsilon)^{d_i} \cdot \prod_{i=k+1}^{r+s} \beta_i(\epsilon)^{d_i} = \beta(\epsilon)\beta'(\epsilon) \Rightarrow \beta(\epsilon)\beta'(\epsilon) = 1.$$

Assim,

$$\beta(\epsilon) = \beta^{-1}(\epsilon), \quad \text{para todo } \epsilon \in \mathcal{O}_{\mathbb{K}}. \quad (4.13)$$

Ainda, para $j = 1, \dots, k$, segue que

$$\beta'(\epsilon_j) = \beta_{k+1}^{d_{k+1}} \dots \beta_{r+s}^{d_{r+s}}(\epsilon_j) = \beta_{k+1}^{d_{k+1}}(\epsilon_j) \dots \beta_{r+s}^{d_{r+s}}(\epsilon_j) \stackrel{Prop. 4.1.16}{\Rightarrow} \beta'(\epsilon_j) < 1.$$

Agora, para $j = k+1, \dots, r+s-1$, segue que

$$\beta(\epsilon_j) = \beta_1^{d_1} \dots \beta_k^{d_k}(\epsilon_j) = \beta_1^{d_1}(\epsilon_j) \dots \beta_k^{d_k}(\epsilon_j) \stackrel{Prop. 4.1.16}{\Rightarrow} \beta(\epsilon_j) < 1.$$

Agora, pelas Equações (4.11) e (4.12), segue que $\prod_{j=1}^{r+s-1} \epsilon_j^{\rho_j} = 1$ e $\beta(1) = \beta'(1) = 1$. Daí,

$$1 = \beta'(1) = \beta' \left(\prod_{j=1}^{r+s-1} \epsilon_j^{\rho_j} \right) = \prod_{j=1}^{r+s-1} \beta(\epsilon_j)^{\rho_j}.$$

Dessa forma, pela Equação (4.13), segue que

$$\prod_{j=1}^k \beta'(\epsilon_j)^{\rho_j} \cdot \prod_{j=k+1}^{r+s-1} \beta' \epsilon_j^{-\rho_j} = 1.$$

No entanto, todos os fatores do lado esquerdo são menores ou iguais a 1 e os primeiros k fatores são estritamente menores do que 1. Portanto, todas as potências devem ser zero e esta é a condição necessária de serem unidades independentes, como queríamos. $\square$

Antes de apresentarmos o próximo resultado, para $j = 1, 2, \dots, r+s-2$, seja

$$a_j = \beta_j(\epsilon_j). \quad (4.14)$$

Dessa forma, pela Proposição 4.1.16, segue que

$$a_j > 1, \quad \text{onde } j = 1, \dots, r+s-1. \quad (4.15)$$

Teorema 4.1.19. *Se $\epsilon \in \mathcal{O}_{\mathbb{K}}$ com*

$$\beta_v(\epsilon) \leq 1, \quad \text{onde } v = 1, 2, \dots, r + s - 1,$$

então existem inteiros $p_1, \dots, p_{r+s-1}$ tais que a unidade

$$\eta = \epsilon \epsilon_1^{p_1} \dots \epsilon_{r+s-1}^{p_{r+s-1}}$$

satisfaz

$$1 < \beta_v(\eta) \leq a_v, \quad \text{onde } v = 1, \dots, r + s - 1, \quad \text{e } \beta_{r+s}(\eta) \leq 1.$$

Demonstração. Se $r + s = 1$, pelo Corolário 4.1.10, segue que

$$\beta_{r+s}(\eta)^{d_{r+s}} = 1,$$

para toda unidade de $\mathcal{O}_{\mathbb{K}}$. Logo,

$$\beta_{r+s}(\eta) = 1,$$

e assim, finalizamos esse caso. Para seguirmos, suponha $r + s \geq 2$ e fixe ϵ uma unidade de $\mathcal{O}_{\mathbb{K}}$ satisfazendo

$$\beta_v(\epsilon), \quad \text{onde } v = 1, 2, \dots, r + s - 1.$$

Consideramos todas unidades η de $\mathcal{O}_{\mathbb{K}}$ da forma

$$\eta = \epsilon \epsilon_1^{k_1} \epsilon_2^{k_2} \dots \epsilon_{r+s-1}^{k_{r+s-1}},$$

com $k_v \geq 0$, $v = 1, \dots, r + s - 1$ e $\beta_v(\eta) \leq a_v$, onde $v = 1, \dots, r + s - 1$. Note que ϵ é uma unidade que satisfaz a Equação (4.15). Para essas unidades, pela Proposição 4.1.16, segue que

$$\beta_{r+s}(\eta) = \beta_{r+s}(\epsilon \epsilon_1^{k_1} \dots \epsilon_{r+s-1}^{k_{r+s-1}}) = \beta_{r+s}(\epsilon) \cdot \prod_{i=1}^{r+s-1} \beta_{r+s}(\epsilon_i)^{k_i} \leq \beta_{r+s}(\epsilon),$$

ou seja, todas as valorizações $\beta_v(\eta)$, onde $v = 1, 2, \dots, r + s$, são limitadas. Portanto, pela Proposição 4.1.8, segue que existe apenas uma quantidade finita de η satisfazendo as hipóteses que definimos. Dentre esses finitos, escolhemos η tais que $\beta_{r+s}(\eta)$ é o menor. Para esse η devemos ter

$$1 < \beta_v(\eta), \quad \text{onde } v = 1, 2, \dots, r + s - 1,$$

uma vez que se para algum $v_0 = 1, \dots, r + s - 1$, então

$$1 \geq \beta_{v_0}(\eta),$$

e para $v = 1, 2, \dots, r + s - 1$, com $v \neq v_0$, então

$$\beta_v(\epsilon_{v_0} \eta) = \beta_v(\epsilon_{v_0}) \beta_v(\eta) < \beta_v(\eta) \leq a_v;$$

Por outro lado, quando $v = v_0$, segue que

$$\beta_{v_0}(\epsilon_{v_0} \eta) = \beta_{v_0}(\epsilon_{v_0}) \beta_{v_0}(\eta) < \beta_{v_0}(\epsilon_{v_0}) \leq a_{v_0};$$

e para $v = r + s$, segue que

$$\beta_{r+s}(\epsilon_{v_0} \eta) = \beta_{r+s}(\epsilon_{v_0}) \beta_{r+s}(\eta) < \beta_{r+s}(\eta),$$

mas isso é um absurdo, uma vez que contradiz a minimalidade de η . Portanto, η é tal que $1 < \beta_v(\eta) \leq a_v$, onde $v = 1, \dots, r + s - 1$ e $\beta_{r+s}(\eta) \leq 1$. $\square$

Corolário 4.1.20. *Existe uma unidade*

$$\epsilon_0 = \epsilon_1^{\sigma_1} \dots \epsilon_{r+s-1}^{r+s-1} \in \mathcal{O}_{\mathbb{K}}$$

com

$$1 < \beta_v(\epsilon_0), \quad \text{onde } v = 1, 2, \dots, r + s - 1.$$

Demonstração. Segue diretamente do Teorema 4.1.19. $\square$

A seguir, vamos fazer o mesmo resultado, mas tirando a hipótese de que $\beta_v(\epsilon) \leq 1$.

Teorema 4.1.21. *Se $\epsilon \in \mathcal{O}_{\mathbb{K}}$, então existe inteiros $\tau_1, \dots, \tau_{r+s-1}$ tais que a unidade*

$$\eta = \epsilon \epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}}$$

satisfaz

$$1 < \beta_v(\eta) \leq a_v, \quad \text{onde } v = 1, \dots, r + s - 1, \quad e \quad \beta_{r+s}(\eta) \leq 1.$$

Demonstração. O caso $r + s = 1$ segue analogamente como na prova do Teorema 4.1.19, isto é,

$$r + s = 1 \Rightarrow \eta = \epsilon \xrightarrow{\text{Cor. 4.1.10}} \beta_{r+s}(\eta)^{d_{r+s}} = 1 \Rightarrow \beta_{r+s}(\eta) = 1.$$

Portanto, suponha $r + s \geq 2$. Seja ϵ uma unidade de $\mathcal{O}_{\mathbb{K}}$. Seja

$$X = \max_{1 \leq v < r+s-1} \beta_v(\epsilon).$$

Pelo Corolário 4.1.20, segue que existe uma unidade

$$\epsilon_0 = \epsilon_1^{\sigma_1} \dots \epsilon_{r+s-1}^{\sigma_{r+s-1}} \in \mathcal{O}_{\mathbb{K}}$$

satisfazendo

$$1 < \beta_v(\epsilon_0), \quad \text{onde } v = 1, 2, \dots, r + s - 1.$$

Seja, também,

$$Y = \min_{1 \leq v \leq r+s-1} \beta_v(\epsilon_0).$$

Logo, $Y > 1$, uma vez que todo $\beta_v(\epsilon_0) > 1$. Agora, devemos escolher $k \in \mathbb{N}$ tal que

$$Y^k \geq X \Rightarrow (\min \beta_v(\epsilon_0))^k \geq \max \beta_v(\epsilon).$$

Assim, $\beta_v(\epsilon_0)^k \geq \beta_v(\epsilon)$, onde $v = 1, 2, \dots, r + s - 1 \Rightarrow 1 \geq \frac{\beta_v(\epsilon)}{\beta_v(\epsilon_0)^k}$. Portanto, a unidade $\lambda = \epsilon \epsilon_0^{-k}$ de $\mathcal{O}_{\mathbb{K}}$ satisfaz

$$\beta_v(\lambda) = \beta_v(\epsilon \epsilon_0^{-k}) = \frac{\beta_v(\epsilon)}{\beta_v(\epsilon_0)^k} \leq 1.$$

Dessa forma, as hipóteses do Teorema 4.1.21 são satisfeitas, e portanto, existem inteiros $\rho_1, \dots, \rho_{r+s-1}$ tais que a unidade

$$\eta = \lambda \epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}}$$

satisfaz

$$1 < \beta_v(\eta) \leq v, \quad \text{onde } v = 1, 2, \dots, r + s - 1.$$

Observe que

$$\eta = \underbrace{\epsilon \epsilon_0^{-k}}_{\lambda} \epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}} = \epsilon \epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}},$$

com $\tau_j = \rho_j - k\sigma_j$, uma vez que

$$\begin{aligned} \epsilon \epsilon_0^{-k} \epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}} &= \epsilon \epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}} \\ \Rightarrow \epsilon_0^{-k} (\epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}}) &= (\epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}}) \\ \Rightarrow (\epsilon_1^{\sigma_1} \dots \epsilon_{r+s-1}^{\sigma_{r+s-1}})^{-k} (\epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}}) &= (\epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}}) \\ \Rightarrow (\epsilon_1^{-k\sigma_1} \dots \epsilon_{r+s-1}^{-k\sigma_{r+s-1}}) (\epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}}) &= (\epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}}) \\ \Rightarrow (\epsilon_1^{-k\sigma_1 + \rho_1} \dots \epsilon_{r+s-1}^{-k\sigma_{r+s-1} + \rho_{r+s-1}}) &= (\epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}}). \end{aligned}$$

Comparando a potência de cada ϵ_j , onde $j = 1, 2, \dots, r+s-1$, segue que $-k\sigma_j + \rho_j = \tau_j$, isto é,

$$\tau_j = \rho_j - k\sigma_j.$$

Finalmente, como $\beta_v(\eta) > 1$, para $v = 1, \dots, r+s-1$, pelo Corolário 4.1.8, segue que

$$\beta_{r+s}(\eta) \leq 1,$$

o que prova o teorema □

Teorema 4.1.22. *Existe apenas uma quantidade finita de unidades $\eta_1, \dots, \eta_h$ de $\mathcal{O}_{\mathbb{K}}$ tais que cada unidade ϵ de $\mathcal{O}_{\mathbb{K}}$ é da forma*

$$\epsilon = \eta_j \epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}}$$

para algum $j \in \{1, \dots, h\}$ e alguns $\rho_1, \dots, \rho_{r+s-1} \in \mathbb{Z}$.

Demonstração. Pelo Teorema 4.1.21, segue que cada unidade ϵ de $\mathcal{O}_{\mathbb{K}}$ pode ser expressa da forma

$$\epsilon = \eta \epsilon_1^{\tau_1} \dots \epsilon_{r+s-1}^{\tau_{r+s-1}},$$

para inteiros $\tau_1, \dots, \tau_{r+s-1}$ e alguma unidade η satisfazendo

$$\beta_v(\eta) \leq a_v, \quad \text{onde } v = 1, 2, \dots, r+s-1; \text{ e } \beta_{r+s}(\eta) \leq 1.$$

Dessa forma, pelo Corolário 4.1.8, segue que existe apenas uma quantidade finita de tal η , digamos, $\eta_1, \dots, \eta_h$. Assim,

$$\epsilon = \eta_j \epsilon_1^{\rho_1} \dots \epsilon_{r+s-1}^{\rho_{r+s-1}},$$

para algum $j \in \{1, \dots, h\}$ e alguns inteiros $\rho_1, \dots, \rho_{r+s-1}$. □

4.2 Teorema das unidades de Dirichlet

Para a demonstração do Teorema das Unidades de Dirichlet (Teorema 4.2.1), além dos resultados da Seção 4.1, precisamos de um teorema sobre decomposição de grupos abelianos finitamente gerados. Como o Teorema 4.2.1 é o resultado mais importante deste trabalho, é pertinente que os detalhes de sua demonstração estejam bem detalhados. Assim, foi feito o apêndice A, onde apresentamos um pouco sobre decomposição de grupos abelianos finitamente gerados, e contém o Teorema fundamental dos grupos abelianos finitamente gerados (A.1.13), resultado utilizado na demonstração do Teorema 4.2.1.

Teorema 4.2.1. (Teorema das Unidades de Dirichlet) *Seja $\mathbb{K}$ um corpo de números de grau $n = r + 2s$, onde r é o número de corpos conjugados reais de $\mathbb{K}$ e $2s$ o número de corpos complexos conjugados de $\mathbb{K}$. Assim, $\mathcal{O}_{\mathbb{K}}$ contém $r + s - 1$ unidades $\epsilon_1, \dots, \epsilon_{r+s-1}$ tais que cada unidade de $\mathcal{O}_{\mathbb{K}}$ pode ser escrita unicamente da forma*

$$\rho \epsilon_1^{n_1} \dots \epsilon_{r+s-1}^{n_{r+s-1}},$$

onde ρ é uma raiz da unidade em $\mathcal{O}_{\mathbb{K}}$ e $n_1, \dots, n_{r+s-1}$ são inteiros.

Demonstração. Considere $U(\mathcal{O}_{\mathbb{K}})$ o grupo que contém todas as unidades de $\mathcal{O}_{\mathbb{K}}$. Pelo Teorema 4.1.22, segue que o grupo das unidades $U(\mathcal{O}_{\mathbb{K}})$ é gerado pelas seguintes unidades

$$\epsilon_1, \dots, \epsilon_{r+s-1}, \eta_1, \dots, \eta_h,$$

isto é,

$$U(\mathcal{O}_{\mathbb{K}}) = \langle \epsilon_1, \dots, \epsilon_{r+s-1}, \eta_1, \dots, \eta_h \rangle.$$

Seja H o subgrupo de $U(\mathcal{O}_{\mathbb{K}})$ dado por

$$H = \langle \epsilon_1, \dots, \epsilon_{r+s-1} \rangle.$$

Ainda, pelo Teorema 4.1.22, segue que existem h classes laterais de H em $U(\mathcal{O}_{\mathbb{K}})$. Logo, o grupo $U(\mathcal{O}_{\mathbb{K}})/H$ tem ordem h . Daí,

$$\epsilon \in U(\mathcal{O}_{\mathbb{K}}) \Rightarrow (\epsilon H)h = H \Rightarrow \epsilon^h \in H.$$

Assim, para cada $\epsilon \in U(\mathcal{O}_{\mathbb{K}})$, existem $a_1, \dots, a_{r+s-1} \in \mathbb{Z}$ tais que

$$\underbrace{\epsilon^j}_{\in H} = \underbrace{\epsilon_1^{a_1} \dots \epsilon_{r+s-1}^{a_{r+s-1}}}_{\text{geradores de } H}$$

Sejam $\lambda_1, \dots, \lambda_m$ unidades de $\mathcal{O}_{\mathbb{K}}$, onde $m \geq r + s$. Assim, para cada um desses λ_i ($i = 1, \dots, m$), segue que existem inteiros $a_{i1}, \dots, a_{i(r+s-1)} \in \mathbb{Z}$ tais que

$$\begin{aligned} \lambda_1^h &= \epsilon_1^{a_{11}} \dots \epsilon_{r+s-1}^{a_{1(r+s-1)}} \\ &\vdots \\ \lambda_m^h &= \epsilon_1^{a_{m1}} \dots \epsilon_{r+s-1}^{a_{m(r+s-1)}}. \end{aligned}$$

Considere o sistema homogêneo de $(r + s - 1)$ equações lineares inteiras com m incógnitas $x_1, \dots, x_m$:

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \dots + a_{m1}x_m = 0 \\ a_{12}x_1 + a_{22}x_2 + \dots + a_{m2}x_m = 0 \\ \vdots \\ a_{1(r+s-1)}x_1 + a_{2(r+s-1)}x_2 + \dots + a_{m(r+s-1)}x_m = 0. \end{cases} \quad (4.16)$$

Como tomamos $m \geq r + s$, segue que $m > r + s - 1$. Logo, o sistema 4.16 tem uma solução $(x_1, \dots, x_m) \in \mathbb{Q}^m$, com $(x_1, \dots, x_m) \neq (0, \dots, 0)$. Multiplicando cada x_i pelo mínimo múltiplo comum de denominadores de $x_1, \dots, x_m$, segue que podemos supor que $(x_1, \dots, x_m) \in \mathbb{Z}^m$. Assim,

$$\begin{aligned} \lambda_1^{hx_1} \dots \lambda_m^{hx_m} &= (\epsilon_1^{a_{11}} \dots \epsilon_{r+s-1}^{a_{1(r+s-1)}})^{hx_1} \dots (\epsilon_1^{a_{m1}} \dots \epsilon_{r+s-1}^{a_{m(r+s-1)}})^{hx_m} \\ &= (\epsilon_1^{h(a_{11}x_1 + \dots + a_{m1}x_m)} \dots \epsilon_{r+s-1}^{h(a_{1(r+s-1)}x_1 + \dots + a_{m(r+s-1)}x_m)}) \\ &\stackrel{(4.8)}{=} \epsilon_1^0 \dots \epsilon_{r+s-1}^0 = 1. \end{aligned}$$

Isso prova que quaisquer m unidades de $\mathcal{O}_{\mathbb{K}}$ com $m \geq r + s$ não são independentes. Portanto, não existe mais do que $r + s - 1$ unidades independentes em $\mathcal{O}_{\mathbb{K}}$. Mas, pelo Teorema 4.1.18, segue que as $(r + s - 1)$ unidades $\epsilon_1, \dots, \epsilon_{r+s-1}$ são independentes.

Agora, pelo *Teorema Fundamental dos grupos abelianos finitamente gerados* (Teorema A.1.13), segue que $U(\mathcal{O}_{\mathbb{K}})$ é o produto direto de grupos cíclicos, $(r + s - 1)$ dos quais tem ordem infinita e os restantes tem ordem finita. A parte livre é $\prod \mathbb{Z}$, e portanto, é infinito. Os elementos de um grupo cíclico de ordem finita, porém, são raízes da unidade. Dessa forma, provamos que toda unidade de $\mathcal{O}_{\mathbb{K}}$ pode ser expressa na forma $\eta \epsilon_1^{x_1} \dots \epsilon_{r+s-1}^{x_{r+s-1}}$, onde η é uma raiz da unidade e cada x_i é inteiro. Por fim, resta mostrar a unicidade, isto é, que essa representação é única. Suponha

$$\eta \epsilon_1^{x_1} \dots \epsilon_{r+s-1}^{x_{r+s-1}} = \theta \eta \epsilon_1^{y_1} \dots \epsilon_{r+s-1}^{y_{r+s-1}}, \quad (4.17)$$

onde η e θ são raízes da unidade e $x_i, y_i \in \mathbb{Z}$, com $i = 1, \dots, r + s - 1$. Assim,

$$\eta \theta^{-1} = \epsilon_1^{y_1 - x_1} \dots \epsilon_{r+s-1}^{y_{r+s-1} - x_{r+s-1}}.$$

Como η e θ são raízes da unidade, então $\eta \theta^{-1}$ também será. Portanto, existe $k \in \mathbb{Z}_+$ tal que

$$(\eta \theta^{-1})^k = 1.$$

Isso implica que

$$\epsilon_1^{y_1 - x_1} \dots \epsilon_{r+s-1}^{y_{r+s-1} - x_{r+s-1}} = 1.$$

Mas, lembre que $\epsilon_1, \dots, \epsilon_{r+s-1}$ são independentes, e pela definição,

$$k(y_1 - x_1) = \dots = k(y_{r+s-1} - x_{r+s-1}) = 0.$$

Logo,

$$y_1 = x_1, \dots, y_{r+s-1} = x_{r+s-1}.$$

Substituindo no sistema (4.17), segue que

$$\eta \epsilon_1^{x_1} \dots \epsilon_{r+s-1}^{x_{r+s-1}} = \theta \eta \epsilon_1^{y_1} \dots \epsilon_{r+s-1}^{y_{r+s-1}} \xrightarrow{x_i = y_i} \eta \epsilon_1^{x_1} \dots \epsilon_{r+s-1}^{x_{r+s-1}} = \theta \epsilon_1^{x_1} \dots \epsilon_{r+s-1}^{x_{r+s-1}} \Rightarrow \eta = \theta.$$

Assim, garantimos a unicidade e finalizamos a prova do teorema. $\square$

4.3 Sistema de unidades fundamentais

Seja $\mathbb{K}$ um corpo de números de grau n com r imersões reais e $2s$ imersões complexas, de modo que $n = r + 2s$.

Definição 4.3.1. Se $\epsilon_1, \dots, \epsilon_{r+s-1}$ são $r + s - 1$ unidades de $\mathcal{O}_{\mathbb{K}}$ tais que

$$\epsilon_1, \dots, \epsilon_{r+s-1} \quad (4.18)$$

são independentes e toda unidade ϵ de $\mathcal{O}_{\mathbb{K}}$ pode ser expressa da forma

$$\epsilon = \eta \epsilon_1^{a_1} \dots \epsilon_{r+s-1}^{a_{r+s-1}}, \quad (4.19)$$

onde η é uma raiz da unidade em $\mathbb{K}$, então $\{\epsilon_1, \dots, \epsilon_{r+s-1}\}$ é chamado **sistema de unidades fundamentais** de $\mathcal{O}_{\mathbb{K}}$.

Note que pelo Teorema das Unidades de Dirichlet (4.2.1) podemos garantir a existência, uma vez que $\mathcal{O}_{\mathbb{K}}$ sempre irá possuir um sistema de unidades fundamentais para qualquer corpo de números $\mathbb{K}$. Ainda, a representação (4.19) de uma unidade em termos do sistema de unidades fundamentais é única pelo argumento final da demonstração do teorema.

Agora, encontremos os sistemas de unidades fundamentais para alguns casos. Se $r + s = 1$, então o sistema de unidades fundamentais é vazio, uma vez que iria conter $r + s - 1 = 1 - 1 = 0$ unidades. Logo, toda unidade de $\mathcal{O}_{\mathbb{K}}$ é uma raiz da unidade. O próximo teorema diz para quais corpos isso ocorre.

Teorema 4.3.2. *Se $\mathbb{K}$ é um corpo de números algébrico, então toda unidade em $\mathcal{O}_{\mathbb{K}}$ é uma raiz da unidade se, e somente se, $\mathbb{K} = \mathbb{Q}$ ou $\mathbb{K}$ é um corpo quadrático imaginário.*

Demonstração. Seja $\mathbb{K}$ um corpo de números de grau n . Seja r o número de imersões reais de $\mathbb{K}$ e $2s$ o número de imersões complexas, de modo que $n = r + 2s$. Pelo Teorema das Unidades de Dirichlet, segue que uma unidade ϵ em $\mathcal{O}_{\mathbb{K}}$ é uma raiz da unidade ρ se, e somente se,

$$\epsilon = \rho \underbrace{\epsilon_1^{n_1} \cdots \epsilon_{r+s-1}^{n_{r+s-1}}}_{=1} \Leftrightarrow r + s - 1 = 0 \Leftrightarrow r + s = 1$$

se, e somente se,

$$\begin{cases} r = 1 & \text{e} & s = 0 & \text{ou} \\ r = 0 & \text{e} & s = 1. \end{cases}$$

Se $r = 1$ e $s = 0$, então $n = 1$, e assim, $\mathbb{K} = \mathbb{Q}$. Agora, se $r = 0$ e $s = 1$, então $n = 2s = 2$ e $\mathbb{K}$ é um corpo quadrático imaginário. $\square$

O Teorema 4.3.2 é consistente com o que já sabemos, isto é,

$$U(\mathcal{O}_{\mathbb{K}}) = U(\mathbb{Z}) = \{\pm 1\}$$

e para m livre de quadrados e negativos, pelo 3.1.1,

$$U(\mathcal{O}_{\mathbb{Q}(\sqrt{m})}) = \begin{cases} \{\pm 1, \pm i\}, & \text{se } m = -1; \\ \{\pm 1, \pm \omega, \pm \omega^2\}, & \text{se } m = -3; \\ \{\pm 1\}, & \text{caso contrário.} \end{cases}$$

onde ω é uma raiz cúbica complexa da unidade.

Se $r + s = 2$, então o sistema de unidades fundamentais consiste em exatamente uma unidade.

Corolário 4.3.3. *Seja $\mathbb{K}$ um corpo de números com $r + s = 2$. O sistema de unidades fundamentais é dado por $\{\epsilon\}$ e, dessa forma, a unidade $\epsilon \in \mathcal{O}_{\mathbb{K}}$ é dita unidade fundamental.*

Observe que no Capítulo 3 já vimos que os corpos quadráticos reais são um caso particular do corolário 4.3.3. Mas o resultado acima é uma generalização. O Teorema 4.3.4 fornece quais corpos possuem uma unidade fundamental.

Se ϵ é uma unidade fundamental de $\mathcal{O}_{\mathbb{K}}$, então toda unidade de $\mathcal{O}_{\mathbb{K}}$ é expressa unicamente da forma $\eta \epsilon^k$, onde η é uma raiz da unidade em $\mathcal{O}_{\mathbb{K}}$ e $k \in \mathbb{Z}$. Mais ainda, sejam ϵ_1 e ϵ_2 duas unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$. Pela aplicação do Teorema das Unidades de Dirichlet, segue que $\epsilon_2 = \lambda \epsilon_1$ ou $\epsilon_1 = \lambda \epsilon_2^{-1}$, para alguma raiz da unidade λ em $\mathcal{O}_{\mathbb{K}}$.

Teorema 4.3.4. *Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K}$ possui uma unidade fundamental se, e somente se, $\mathbb{K}$ é um corpo quadrático real, um corpo cúbico com exatamente uma imersão real ou um corpo quártico totalmente imaginário.*

Demonstração. Seja $\mathbb{K}$ um corpo de números de grau n . Sejam r o número de imersões reais de $\mathbb{K}$ e $2s$ o número de imersões complexas. Pelo Teorema 4.2.1, segue que $U(\mathcal{O}_{\mathbb{K}})$ possui uma unidade fundamental se, e somente se, $r + s = 2$. Para este caso, 3 opções podem ocorrerem.

1. $r = 2$ e $s = 0 \Rightarrow n = 2 \Rightarrow \mathbb{K}$ é um corpo quadrático totalmente real.
2. $r = 1$ e $s = 1 \Rightarrow n = 3 \Rightarrow \mathbb{K}$ é um corpo cúbico com apenas uma imersão real.
3. $r = 0$ e $s = 2 \Rightarrow n = 4 \Rightarrow \mathbb{K}$ é um corpo quártico totalmente imaginário.

Com isso, o teorema está provado. $\square$

4.4 Raízes da unidade contidas em $\mathcal{O}_{\mathbb{K}}$

Os teoremas dessa seção fornecem informações sobre quais raízes da unidade podem pertencer ao anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números $\mathbb{K}$. Lembre, primeiramente que, pela Teoria de Galois, se ξ_k é uma raiz primitiva da unidade, então

$$[\mathbb{Q}(\xi_k) : \mathbb{Q}] = \varphi(k), \quad (4.20)$$

onde φ é a função de Euler.

Para darmos continuidade, provamos alguns resultados elementares sobre a função φ de Euler que serão úteis para as demonstrações dos teoremas dando informações sobre as raízes da unidade em anéis de inteiros de um corpo de números algébrico.

Definição 4.4.1. A função $\varphi : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$ que associa cada $n \in \mathbb{N} \setminus \{0\}$ ao número de elementos de $\{k \in \mathbb{N} \setminus \{0\} \mid 1 \leq k \leq n \text{ e } \text{mdc}(k, n) = 1\}$ é chamada **função φ de Euler**.

Teorema 4.4.2. *Se p é um primo e k um inteiro positivo, então*

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Demonstração. Como entre 1 e p^k os únicos elementos não primos com p^k são

$$p, 2p, 3p, \dots, (p^{k-1})p,$$

segue que existem p^{k-1} não primos com p . Portanto,

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right),$$

o que prova o teorema. $\square$

Corolário 4.4.3. *p é um primo se, e somente se, $\varphi(p) = p - 1$.*

Demonstração. Seja p um primo. Como de 1 a p o único elemento não primo com p é o próprio p , segue que $\varphi(p) = p - 1$. Reciprocamente, se p não é um primo, então p teria pelo menos um divisor d tal que $1 < d < p$. Assim, no mínimo dois inteiros entre 1 e p não seriam primos com p . Portanto, $\varphi(p) \leq p - 2$, o que é uma contradição. Assim, p é um primo. $\square$

Proposição 4.4.4. *Se m e n são números naturais não nulos e primos entre si, então $\varphi(mn) = \varphi(m)\varphi(n)$, ou seja, a função φ de Euler é multiplicativa.*

Demonstração. Seja a seguinte tabela formada por todos os naturais de 1 a mn

1	2	3	...	h	...	n
n+1	n+2	n+3	...	n+h	...	2n
2n+1	2n+2	2n+3	...	2n+h	...	3n
$\vdots$	$\vdots$	$\vdots$	...	$\vdots$	...	$\vdots$
(m-1)n+1	(m-1)n+2	(m-1)n+3	...	(m-1)n+h	...	mn

Como $\text{mdc}(qn + h, n) = \text{mdc}(h, n)$, segue que os inteiros da h -ésima coluna são primos com n se, e somente se, h é primo com n . Mas, na primeira linha o número de inteiros que são primos com n é $\varphi(n)$, e deste modo, existem somente $\varphi(n)$ colunas formadas com inteiros que são primos com n . Por outro lado, em cada uma dessas $\varphi(n)$ colunas existem $\varphi(m)$ elementos que são primos com m . Assim, o número total de inteiros que são primos com n e com m , ou seja, o número de primos com mn é exatamente $\varphi(m)\varphi(n)$, ou seja,

$$\varphi(mn) = \varphi(m)\varphi(n),$$

o que prova a proposição. $\square$

Teorema 4.4.5. *Se $n > 1$ é um inteiro cuja decomposição em primos é $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, então $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$.*

Demonstração. Pelo Teorema 4.4.2, segue que

$$\varphi(p_i^{k_i}) = p_i^{k_i} \left(1 - \frac{1}{p_i}\right).$$

Como φ é multiplicativa, segue que

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_r^{k_r}) = p_1^{k_1} \left(1 - \frac{1}{p_1}\right) p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \dots p_r^{k_r} \left(1 - \frac{1}{p_r}\right) \\ &= p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right), \end{aligned}$$

o que prova o teorema. $\square$

Observação 4.4.6. Uma maneira equivalente de escrever a expressão do Teorema 4.4.5 é $\varphi(k) = p_1^{k_1-1} \dots p_r^{k_r-1} (p_1 - 1) \dots (p_r - 1)$. Nos resultados, a seguir, usamos a que for mais conveniente.

Usando as propriedades da função de Euler juntamente com as decomposições de potências de primos de inteiros positivos até 45, a seguir apresentamos os valores de $\varphi(k)$, para $k = 1, \dots, 45$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varphi(k)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

k	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\varphi(k)$	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

k	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
$\varphi(k)$	30	16	20	16	24	12	36	18	24	16	40	12	42	20	24

Tabela 4.1: Valores da função de Euler $\varphi(k)$ para $k \leq 45$.

Proposição 4.4.7. *Se n é um inteiro positivo, então*

$$\varphi(n) \geq \sqrt{\frac{n}{2}}.$$

Demonstração. Se p é um primo ímpar e k é um inteiro positivo, então

$$\varphi(p^k) = \begin{cases} p - 1 \geq p^{\frac{1}{2}}, & \text{se } k = 1; \\ p^{k-1}(p - 1) > p^{k-1} \geq p^{\frac{1}{2}}, & \text{se } k \geq 2. \end{cases}$$

Assim,

$$\varphi(p^k) \geq \sqrt{p^k}.$$

Logo, se n é um inteiro positivo ímpar, como φ é multiplicativa, segue que

$$\varphi(n) \geq \sqrt{n}.$$

Seja m um inteiro positivo. Seja $m = 2^\alpha n$, onde α é um inteiro não negativo e n é um inteiro positivo ímpar. Se $\alpha = 0$ ou $\alpha = 1$, então

$$\varphi(m) = \varphi(n) \geq \sqrt{n} \geq \sqrt{\frac{n}{2}}.$$

Se $\alpha \geq 2$, então

$$\varphi(m) = 2^{\alpha-1} \varphi(n) \geq 2^{\frac{\alpha}{2}} \varphi(n) \geq 2^{\frac{\alpha}{2}} \sqrt{n} = \sqrt{m}.$$

Dessa forma,

$$\varphi(m) \geq \sqrt{\frac{n}{2}}, \quad \text{para todo } n \geq 0, \quad n \in \mathbb{Z},$$

o que prova a proposição. □

Proposição 4.4.8. *Seja n um inteiro positivo. Se $\varphi(k) \leq n$, então $k \leq 2n^2$.*

Demonstração. Pela Proposição 4.4.7, segue que

$$\sqrt{\frac{k}{2}} \leq \varphi(k) \leq n \Rightarrow \frac{1}{2} \leq n^2 \Rightarrow k \leq 2n^2,$$

o que prova a proposição. $\square$

Proposição 4.4.9. $\varphi(k) = 1$ se, e somente se, $k = 1$ ou $k = 2$.

Demonstração. Pela Proposição 4.4.8, segue que $\varphi(k) = 1 \Rightarrow k \leq 2.1^2 = 1 \Rightarrow k = 1$ ou $k = 2$. Conferindo a Tabela 4.4, vemos que ambos valores satisfazem $\varphi(k) = 1$. $\square$

Proposição 4.4.10. $\varphi(k) = 2$ se, e somente se, $k = 3, 4, 6$.

Demonstração. Pela Proposição 4.4.8, segue que $\varphi(k) = 2 \Rightarrow k \leq 2.2^2 = 8$. Assim, existem 8 opções para k . Entretanto, conferindo a Tabela 4.4, obtemos os seguintes valores:

k	1	2	3	4	5	6	7	8
$\varphi(k)$	1	1	2	2	4	2	6	4

Logo, $\varphi(k) = 2 \Leftrightarrow k = 3, 4, 6$. $\square$

Proposição 4.4.11. $\varphi(k) = 4$ se, e somente se, $k = 5, 8, 10, 12$.

Demonstração. Pela Proposição 4.4.8, segue que $\varphi(k) = 4 \Rightarrow k \leq 2.4^2 = 2.16 = 32$. Mais uma vez, conferimos os valores de $k \leq 32$ na Tabela 4.4. Agora, o resultado segue do fato de que $\varphi(k) = 4$, para $k = 5, 8, 10, 12$. $\square$

Proposição 4.4.12. Se $n \geq 3$, então $\varphi(n)$ é par.

Demonstração. Se $n \geq 3$, então existe um primo p ímpar dividindo n ou $n = 2^\alpha$ com $\alpha \geq 2$. No primeiro caso, $n = p^\beta \cdot n_1$, onde $\beta \geq 1$ e n_1 não é divisível por p . Assim,

$$\varphi(n) = p^{\beta-1}(p-1) \cdot \varphi(n_1) \equiv 0 \pmod{2},$$

uma vez que $2 \mid p-1$. No segundo caso,

$$\varphi(n) = 2^{\alpha-1} \equiv 0 \pmod{2}, \quad \text{onde } \alpha \geq 2.$$

Portanto,

$$n \geq 3 \Rightarrow \varphi(n) = 2k, \quad \text{com } k \geq 1,$$

o que prova a proposição. $\square$

Agora, usando os resultados anteriores, mostramos que o anel de inteiros de um corpo de números contém apenas uma quantidade finita de raízes da unidade.

Teorema 4.4.13. Se $\mathbb{K}$ é um corpo de números, então $\mathcal{O}_{\mathbb{K}}$ contém apenas uma quantidade finita de raízes da unidade.

Demonstração. Considere $[\mathbb{K} : \mathbb{Q}] = n$. Se ξ_k é uma raiz k -ésima primitiva da unidade em $\mathcal{O}_{\mathbb{K}}$, então $\xi_k \in \mathbb{K}$, e portanto,

$$\mathbb{Q}(\xi_k) \subseteq \mathbb{K}.$$

Logo,

$$[\mathbb{Q}(\xi_k) : \mathbb{K}] \leq [\mathbb{K} : \mathbb{Q}],$$

isto é, $\varphi(k) \leq n$. Pela Proposição 4.4.8, segue que $k \in \{1, 2, \dots, 2n^2\}$. Portanto, existe apenas uma quantidade finita de raízes ξ_k da unidade em $\mathcal{O}_{\mathbb{K}}$. $\square$

Se $\mathbb{K}$ tem grau ímpar, então podemos dizer exatamente quais raízes da unidade estão em $\mathcal{O}_{\mathbb{K}}$.

Teorema 4.4.14. *Se $\mathbb{K}$ é um corpo de números de grau ímpar n , então as únicas raízes da unidade em $\mathcal{O}_{\mathbb{K}}$ são ± 1 .*

Demonstração. Se ξ_k uma raiz k -ésima primitiva da unidade em $\mathcal{O}_{\mathbb{K}}$, então $\mathbb{Q}(\xi_k) \subseteq \mathbb{K}$, e portanto, $[\mathbb{Q}(\xi_k) : \mathbb{K}] \mid [\mathbb{K} : \mathbb{Q}]$, isto é, $\varphi(k) \mid n$. Como n é ímpar, segue que $\varphi(k)$ também é ímpar. Assim, pela Proposição 4.4.12, segue que $k \leq 2$, isto é, $k = 1$ ou $k = 2$. Desse modo, $\xi_1 = 1$ e $\xi_2 = -1$ pertencem a $\mathcal{O}_{\mathbb{K}}$. $\square$

Corolário 4.4.15. *As únicas raízes da unidade no anel de inteiros de um corpo cúbico são ± 1 .*

Demonstração. Tomando $n = 3$ no Teorema 4.4.14, segue o resultado. $\square$

Agora, analisamos quando n é par. Nestes casos, a situação é mais complexa. Neste trabalho, apenas determinamos as raízes da unidade no anel de inteiros de um corpo quadrático.

Teorema 4.4.16. *Se $\mathbb{K}$ é um corpo quadrático, então as únicas possibilidades de raízes da unidade $\neq \pm 1$ em $\mathcal{O}_{\mathbb{K}}$ são*

$$\xi_3, \xi_4, \xi_5, \xi_6, \xi_8, \xi_{10}, \xi_{12}$$

e suas potências. Mais precisamente,

$$\begin{aligned} \xi_3 \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(\sqrt{-3}), \\ \xi_4 \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(\sqrt{-1}), \\ \xi_5 \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} = \mathbb{Q}(\sqrt{-10 - 2\sqrt{5}}), \\ \xi_6 \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(\sqrt{-3}), \\ \xi_8 \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} = \mathbb{Q}(\sqrt{\sqrt{2}, \sqrt{-1}}), \\ \xi_{10} \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} = \mathbb{Q}(\sqrt{-10 - 2\sqrt{5}}), \\ \xi_{12} \in \mathcal{O}_{\mathbb{K}} &\Leftrightarrow \mathbb{K} = \mathbb{Q}(\sqrt{\sqrt{3}, \sqrt{-1}}). \end{aligned}$$

Demonstração. Se ξ_k é uma k -ésima raiz primitiva da unidade em $\mathcal{O}_{\mathbb{K}}$, então $\mathbb{Q}(\xi_k) \subseteq \mathbb{K} \Rightarrow [\mathbb{Q}(\xi_k) : \mathbb{Q}] \mid [\mathbb{K} : \mathbb{Q}] \Rightarrow [\mathbb{K} : \mathbb{Q}] = 4 \Rightarrow [\mathbb{Q}(\xi_k) : \mathbb{Q}] = \varphi(k) \mid 4 \Rightarrow \varphi(k) = 1, 2, 3$ ou 4 . Pelas Proposições 4.4.9, 4.4.10 e 4.4.11, segue as seguintes opções para k :

$$k = \underbrace{1, 2}_{\varphi(k)=1}, \underbrace{3, 4, 6}_{\varphi(k)=2} \text{ ou } \underbrace{5, 8, 10, 12}_{\varphi(k)=4}.$$

Dessa forma, as únicas possíveis raízes da unidade em $\mathcal{O}_{\mathbb{K}}$ são ξ_i , onde $i = 1, 2, 3, 4, 5, 6, 8, 10, 12$, e suas potências. Quando $\varphi(k) = 1$, obtemos ξ_1 e ξ_2 , e já sabemos que $\xi_1 = 1$ e $\xi_2 = -1$. Como queremos os valores diferentes desses, analisamos as outras possibilidades. Lembre primeiramente que, para uma raiz k -ésima da unidade,

$$\xi^k = 1 \Leftrightarrow \xi_k = e^{\frac{2\pi i}{k}} = \cos\left(\frac{2\pi}{k}\right) + i \operatorname{sen}\left(\frac{2\pi}{k}\right).$$

Tendo isso em vista, vejamos para cada índice restante.

1. Se $k = 3$, então

$$\xi_3 = e^{\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) + i \operatorname{sen}\left(\frac{2\pi}{3}\right) = \frac{1}{2} + i\frac{\sqrt{3}}{3},$$

e assim,

$$\mathbb{Q}(\xi_3) = \mathbb{Q}(e^{\frac{2\pi i}{3}}) = \mathbb{Q}(\sqrt{3}i) = \mathbb{Q}(\sqrt{-3}).$$

Portanto, $\xi_3 \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(xi_3) = \mathbb{Q}(\sqrt{-3})$.

2. Se $k = 4$, então

$$\xi_4 = e^{\frac{2\pi i}{4}} = \cos\left(\frac{2\pi}{4}\right) + i \operatorname{sen}\left(\frac{2\pi}{4}\right) = \cancel{\cos\left(\frac{\pi}{2}\right)} + i \operatorname{sen}\left(\frac{\pi}{2}\right) = i,$$

e assim,

$$\mathbb{Q}(\xi_4) = \mathbb{Q}(\sqrt{-1}).$$

Portanto, $\xi_4 \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(xi_4) = \mathbb{Q}(\sqrt{-1})$.

3. Se $k = 6$, então

$$\xi_6 = e^{\frac{2\pi i}{6}} = \cos\left(\frac{2\pi}{6}\right) + i \operatorname{sen}\left(\frac{2\pi}{6}\right) = \cos\left(\frac{\pi}{3}\right) + i \operatorname{sen}\left(\frac{\pi}{3}\right) = \frac{1}{2} + i\frac{\sqrt{3}}{2},$$

e assim,

$$\mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{-3}).$$

Portanto, $\xi_3 \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{-3})$.

Assim, fechamos as possibilidades para $\varphi(k) = 2$; Por fim, vejamos para $\varphi(k) = 4$.

1. Se $k = 5$, então

$$\begin{aligned} \xi_5 &= e^{\frac{2\pi i}{5}} = \cos\left(\frac{2\pi}{5}\right) + i \operatorname{sen}\left(\frac{2\pi}{5}\right) = \frac{-1+\sqrt{5}}{4} + i\frac{\sqrt{10-2\sqrt{5}}}{4} \\ &= \frac{1}{4}(\sqrt{5} - 1 + i\sqrt{10 - 2\sqrt{5}}), \end{aligned}$$

e assim, $\mathbb{Q}(\xi_5) = \mathbb{Q}(\sqrt{-10 - 2\sqrt{5}})$. Logo,

$$\xi_5 \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \subseteq \mathbb{Q}(\xi_5) = \mathbb{Q}(\sqrt{-10 - 2\sqrt{5}}).$$

Mas, note que $[\mathbb{Q}(\xi_5) : \mathbb{Q}] = \varphi(k) = \varphi(5) = 4 = [\mathbb{K} : \mathbb{Q}]$. Dessa forma, $\mathbb{K} = \mathbb{Q}(\sqrt{-10 - 2\sqrt{5}})$.

2. Se $k = 8$, então

$$\xi_8 = e^{\frac{2\pi i}{8}} = \cos\left(\frac{\pi}{4}\right) + i \sin\left(\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2},$$

e assim,

$$\mathbb{Q}(\xi_4) = \mathbb{Q}(\sqrt{2}, \sqrt{-1}).$$

Portanto, $\xi_8 \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \in \mathbb{Q}(\xi) \stackrel{\varphi(k)=4=n}{\Leftrightarrow} \mathbb{K} = \mathbb{Q}(\sqrt{-2})$.

3. Se $k = 10$, então

$$\xi_{10} = e^{\frac{2\pi i}{10}} = \cos\frac{\pi}{5} + i \sin\frac{\pi}{5} = \frac{\sqrt{5}+1}{4} + i \frac{\sqrt{10+2\sqrt{5}}}{4},$$

e assim,

$$\mathbb{Q}(\xi_{10}) = \mathbb{Q}\left(\sqrt{-10-2\sqrt{5}}\right).$$

Mas, $[\mathbb{Q}(\xi_k) : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}] = n$.

Portanto, $\xi_{10} \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \in \mathbb{Q}(\xi_{10}) \Leftrightarrow \mathbb{K} = \mathbb{Q}\left(\sqrt{-10-2\sqrt{5}}\right)$.

4. Se $k = 12$, então

$$\xi_{12} = e^{\frac{2\pi i}{12}} = \cos\left(\frac{\pi}{6}\right) + i \sin\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} + i \frac{1}{2},$$

e assim,

$$\mathbb{Q}(\xi_{12}) = \mathbb{Q}(\sqrt{3}, -1).$$

Portanto, $\xi_{12} \in \mathcal{O}_{\mathbb{K}} \Leftrightarrow \mathbb{K} \in \mathbb{Q}(\xi_{12}) \Leftrightarrow \mathbb{Q}(\xi_{12}) = \mathbb{Q}(\sqrt{3}, -1)$,

o que prova o teorema. $\square$

Exemplo 4.4.17. Existe uma quantidade infinita de corpos quadráticos $\mathbb{K}$ tal que $\xi_4 \in \mathcal{O}_{\mathbb{K}}$. Considere

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\},$$

o conjunto dos números primos. Já é sabido que existem infinitos números primos, e portanto, $\mathbb{P}$ é infinito. Ainda, para $p \in \mathbb{P}$, considere

$$\mathbb{K}_p = \mathbb{Q}(\sqrt{-1}, \sqrt{p}).$$

Assim,

$$[\mathbb{K}_p : \mathbb{Q}] = 4, \text{ para todo } p \in \mathbb{P}.$$

Mais ainda, os únicos subcorpos quadráticos de $\mathbb{K}_p$, onde $p \in \mathbb{P}$, são

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{p}) \text{ e } \mathbb{Q}(\sqrt{-p}).$$

Considere, agora, $p, q \in \mathbb{P}$ tal que $p \neq q$. Assim, $\mathbb{Q}(\sqrt{q})$ é um subcorpo quadrático de $\mathbb{K}_q$, mas não de $\mathbb{K}_p$, uma vez que $\mathbb{Q}(\sqrt{q}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{-p})$. Portanto, $K_q \neq K_p$. Como $\mathbb{P}$ é infinito, segue que $\{\mathbb{K}_p \mid p \in \mathbb{P}\}$ é conjunto infinito de corpos quadráticos distintos, onde todos contêm K_p pelo Teorema 4.4.16.

Exemplo 4.4.18. Existe uma quantidade infinita de corpos quadráticos $\mathbb{K}$ tal que as únicas raízes da unidade dos seus anéis de inteiros $\mathcal{O}_{\mathbb{K}}$ é ± 1 . Considere

$$\mathbb{P}_{3,4} = \{3, 7, 11, 19, 23, 31, \dots\}$$

o conjunto dos números primos p tal que $p \equiv 3 \pmod{4}$. Para todo $p \in \mathbb{P}$, sejam

$$\sigma_p = \sqrt{1 + \sqrt{p}} \text{ e } \mathbb{K}_p = \mathbb{Q}(\sigma_p).$$

Assim, σ_p é uma raiz do polinômio

$$f_p(x) = x^4 - 2x^2 + (1 - p) \in \mathbb{Z}[x].$$

Como $2 \mid (1 - p)$, para todo $p \in \mathbb{P}_{3,4}$, segue que $f_p(x)$ é irredutível em $\mathbb{Z}[x]$ pelo critério de Eisenstein para $p = 2$. Desse modo, f_p é o polinômio minimal de σ_p sobre $\mathbb{Q}$, e portanto, $[\mathbb{K}_p : \mathbb{Q}] = 4$. Se $q \in \mathbb{P}_{3,4}$ é tal que $p \neq q$, é fácil ver que $\sqrt{q} \notin \mathbb{K}_p$. Mas, $\sqrt{q} \in \mathbb{K}_q$, e assim, $\mathbb{K}_p \neq \mathbb{K}_q$. Consequentemente, como há infinitos números primos tais que $p \equiv 3 \pmod{4}$, o conjunto $\{\mathbb{K}_p \mid p \in \mathbb{P}_{3,4}\}$ possui infinitos corpos quadráticos. Ainda, como $\mathbb{K}_p \subseteq \mathbb{R}$, nenhuma das raízes da unidade ξ_k , $k \in \{3, 4, 5, 6, 8, 10, 12\}$, pertence a $\mathcal{O}_{\mathbb{K}}$. Assim, pelo Teorema 4.4.16, as únicas raízes da unidade em $\mathcal{O}_{\mathbb{K}}$ são ± 1 .

4.5 Unidades em corpos cúbicos

Seja $\mathbb{K}$ um corpo cúbico com apenas uma imersão real. Para analisarmos as Unidades em Corpos Cúbicos, vamos relembrar alguns resultados. Pelo Teorema 4.3.4, sabemos que $\mathbb{K}$ possui uma unidade fundamental η . Suponha ainda que $\mathbb{K}$ é um corpo totalmente real, então nesse caso $\eta \in \mathbb{R}$. Pelo Teorema 4.4.14, as únicas raízes da unidade de $\mathbb{K}$ são ± 1 . Consequentemente, as únicas unidades fundamentais são $\pm \eta$ e $\pm \eta^{-1}$. Exatamente uma dessas unidades é maior que 1. Portanto, $\mathbb{K}$ possui uma única unidade fundamental $\eta > 1$.

Vamos determinar tal unidade η para quando $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$ e quando $\mathbb{K} = \mathbb{Q}(\sqrt[3]{3})$. A ferramenta principal desta seção será o Teorema 4.5.3, que fornece um limite inferior para a unidade fundamental em termos do discriminante do corpo $\mathbb{K}$. Para a demonstração desse resultado, precisamos de algumas desigualdades que são provadas como Lemas a seguir.

Lema 4.5.1. Se $x \in \mathbb{R}$ e $\theta \in \mathbb{K}$, então

$$\sin^2 \theta (x - 2 \cos \theta)^2 < x^2 + 4.$$

Demonstração. Para todo $\theta \in \mathbb{R}$, segue que

$$1 - \sin^2 \theta \cos^2 \theta - \sin^4 \theta = 1 - \sin^2 \theta (\cos^2 \theta + \sin^2 \theta) = 1 - \sin^2 \theta = \cos^2 \theta \geq 0.$$

Para a igualdade, devemos ter:

$$\cos^2(\theta) = 0 \Leftrightarrow \theta = (2k + 1)\frac{\pi}{2}, \quad k \in \mathbb{Z}.$$

Portanto, para todo $x \in \mathbb{R}$ e todo $\theta \in \mathbb{R}$, segue que

$$(x \cos \theta + 2 \sin^2 \theta)^2 + 4 \underbrace{(1 - \sin^2 \theta \cos^2 \theta - \sin^4 \theta)}_{\cos^2 \theta} > 0. \quad (4.21)$$

Substituindo $\theta = (2k + 1)\frac{\pi}{2}$, com $k \in \mathbb{Z}$, segue que

$$\cancel{x \cdot \cos\left(\frac{(2k+1)\pi}{2}\right)}^0 + \cancel{2 \cdot \sin\left(\frac{(2k+1)\pi}{2}\right)}^1 + \cancel{4 \cdot \cos^2\left(\frac{(2k+1)\pi}{2}\right)}^0 = 2 \cdot 1 = 2.$$

Expandindo o quadrado da Equação (4.21), segue que

$$\begin{aligned} & [(x \cos \theta)^2 + 2 \cdot (x \cdot \cos \theta)(2 \cdot \sin^2 \theta) + (2 \sin^2 \theta)^2] + [4 - 4 \sin^2 \theta \cos^2 \theta - 4 \sin^4 \theta] \\ &= x^2 \cos^2 \theta + 4x \sin^2 \theta \cos \theta + \cancel{4 \sin^4 \theta} + 4 - 4 \sin^2 \theta \cos^2 \theta - \cancel{4 \sin^4 \theta} \\ &= x^2 \cos^2 \theta + (4x \sin^2 \theta \cos \theta) + 4 - (4 \sin^2 \theta \cos^2 \theta) > 0 \end{aligned}$$

se, e somente se,

$$x^2 \cos^2 \theta + 4 > -4x \sin^2 \theta \cos \theta + 4 \sin^2 \theta \cos^2 \theta. \quad (4.22)$$

Se $x^2 \sin^2 \theta > 0$, então podemos somar esse valor em ambos lados da desigualdade (4.21) sem alterá-la. Assim,

$$\begin{aligned} x^2 \sin^2 \theta - 4x \sin^2 \theta \cos \theta + 4 \sin^2 \theta \cos^2 \theta &< x^2 \sin^2 \theta + x^2 \cos^2 \theta + 4 = \\ &\cancel{x^2(\sin^2 \theta + \cos^2 \theta)}^1 + 4 = x^2 + 4. \end{aligned}$$

Por outro lado,

$$\begin{aligned} \sin^2 \theta (x - 2 \cos \theta)^2 &= \sin^2 \theta (x^2 - 4x \cos \theta + 4 \cos^2 \theta) \\ &= x^2 \sin^2 \theta - 4x \sin^2 \theta \cos \theta + 4 \sin^2 \theta \cos^2 \theta < x^2 + 4. \end{aligned}$$

Portanto, para todo $x \in \mathbb{R}$, segue que $\sin^2 \theta (x - 2 \cos \theta)^2 < x^2 + 4$. □

Lema 4.5.2. *Se $x \geq 33$, então*

$$\sqrt{\left(\frac{x}{8} - 3\right)^2 - 1} > \frac{x}{8} - \frac{15}{4}.$$

Demonstração. Primeiro,

$$\begin{aligned} \left(\frac{x}{8} - 3\right)^2 - \left(\frac{x}{8} - \frac{15}{4}\right)^2 &= \left(\left(\frac{x}{8}\right)^2 - 2 \cdot \frac{x}{8} \cdot 3 + 3^2\right) - \left(\left(\frac{x}{8}\right)^2 - 2 \cdot \frac{x}{8} \cdot \frac{15}{4} + \left(\frac{15}{4}\right)^2\right) \\ &= \left(\frac{x}{8}\right)^2 - 6 \cdot \frac{x}{8} + 9 - \left(\frac{x}{8}\right)^2 + \frac{15}{2} \cdot \frac{x}{8} - \frac{225}{16} \\ &= -\frac{12x}{16} + \frac{15x}{16} + \frac{144}{16} - \frac{225}{16} \\ &= \frac{3x}{16} - \frac{81}{16} = \frac{3}{4} \left(\frac{x}{4} - \frac{27}{4}\right). \end{aligned}$$

Se $x = 33$, então

$$\frac{3}{4} \left(\frac{33}{4} - \frac{27}{4}\right) = \frac{3}{4} \cdot \frac{6}{4} = \frac{18}{16} = \frac{9}{8} > 1.$$

Assim, suponha que $x \geq 33$. Daí,

$$\begin{aligned} \frac{3}{4} \left(\frac{x}{4} - \frac{27}{4} \right) &\geq \frac{3}{4} \left(\frac{33}{4} - \frac{27}{4} \right) > 1 \Leftrightarrow \frac{3}{4} \left(\frac{x}{4} - \frac{27}{4} \right) > 1 \Leftrightarrow \\ \left(\frac{x}{8} - 3 \right)^2 - \left(\frac{x}{8} - \frac{15}{4} \right)^2 &> 1 \Leftrightarrow \left(\frac{x}{8} - 3 \right)^2 - 1 > \left(\frac{x}{8} - \frac{15}{4} \right)^2 \Leftrightarrow \\ \sqrt{\left(\frac{x}{8} - 3 \right)^2 - 1} &> \frac{x}{8} - \frac{15}{4}. \end{aligned}$$

Portanto, segue a desigualdade desejada para todo $x \geq 33$. $\square$

Os Lemas 4.5.1 e 4.5.2 fornecem ferramentas para provar o Teorema principal desta seção, que será enunciado a seguir.

Teorema 4.5.3. *Seja $\mathbb{K}$ um corpo cúbico real com duas imersões complexas. Seja $\eta > 1$ a unidade fundamental de $\mathcal{O}_{\mathbb{K}}$. Se $|d(K)| \geq 33$, então*

$$\eta^3 > \frac{|d(K)| - 27}{4}.$$

Demonstração. Seja η a unidade fundamental de $\mathcal{O}_{\mathbb{K}}$. Considere $\rho e^{i\theta}, \rho e^{-i\theta}$ os conjugados de η , onde $\rho \in \mathbb{R}_+$. Como η é uma unidade, segue que

$$N(\eta) = \pm 1.$$

Mas, pela definição de norma de um elemento (Definição 2.3.17), segue que é calculada pelo produto do elemento com seus conjugados. Logo,

$$N(\eta) = \eta \cdot \rho e^{i\theta} \cdot \rho e^{-i\theta} = \pm 1 \Leftrightarrow \eta \rho^2 \frac{e^{i\theta}}{e^{i\theta}} = \pm 1 \Leftrightarrow \eta \rho^2 = \pm 1.$$

Como $\eta > 1$ e $\rho^2 > 0$, segue que

$$\eta \rho^2 = 1.$$

Assim,

$$\eta = \frac{1}{\rho^2} = \rho^{-2}.$$

Agora, vejamos qual é o determinante de η , ou seja,

$$D(\eta) = D(1, \eta, \eta^2) = \begin{vmatrix} 1 & \eta & \eta^2 \\ 1 & \rho e^{i\theta} & \rho^2 e^{2i\theta} \\ 1 & \rho e^{-i\theta} & \rho^2 e^{-2i\theta} \end{vmatrix}^2.$$

Para facilitar a conta, vamos fazer primeiramente apenas o cálculo do determinante. Substituindo η por ρ^2 , segue que

$$D(\eta) = \begin{vmatrix} 1 & \rho^{-2} & \rho^{-4} \\ 1 & \rho e^{i\theta} & \rho^2 e^{2i\theta} \\ 1 & \rho e^{-i\theta} & \rho^2 e^{-2i\theta} \end{vmatrix}.$$

Por ser conveniente, vamos subtrair a primeira linha da segunda e terceira linha do determinante, e assim,

$$\begin{aligned}
 D(\eta) &= \begin{vmatrix} 1 & \rho^{-2} & \rho^{-4} \\ 1 & \rho e^{i\theta} - \rho^{-2} & \rho^2 e^{2i\theta} - \rho^{-4} \\ 1 & \rho e^{-i\theta} - \rho^{-2} & \rho^2 e^{-2i\theta} - \rho^{-4} \end{vmatrix} \\
 &= (\rho e^{i\theta} - \rho^{-2})(\rho^2 e^{-2i\theta} - \rho^{-4}) - (\rho e^{-i\theta} - \rho^{-2})(\rho^2 e^{2i\theta} - \rho^{-4}) \\
 &= \rho^3 e^{i\theta-2i\theta} - \rho^{1-4} e^{i\theta} - \rho^{2-2} e^{-2i\theta} + \rho^{-2-4} - \rho^3 e^{-i\theta+2i\theta} + \rho^{-3} e^{-i\theta} + e^{2i\theta} - \rho^{-6} \\
 &= \rho^3 e^{-i\theta} - \rho^{-3} e^{i\theta} - e^{-2i\theta} + \cancel{\rho^{-6}} - \rho^3 e^{i\theta} + \rho^{-3} e^{-i\theta} + e^{2i\theta} - \cancel{\rho^{-6}} \\
 &= \rho^3(e^{-i\theta} - \eta^{i\theta}) + (-e^{-2i\theta} + e^{2i\theta}) + \rho^{-3}(-e^{i\theta} + e^{-i\theta}) \\
 &= -\rho^3(e^{i\theta} - \eta^{-i\theta}) + (e^{i\theta} - e^{-i(2\theta)}) + \rho^{-3}(-e^{i\theta} + e^{-i\theta}) - \rho^{-3}(e^{i\theta} - e^{-i\theta}).
 \end{aligned}$$

Usamos agora uma igualdade muito conhecida, a fórmula de Euler,

$$\sin \theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Voltando de onde paramos no cálculo do determinante,

$$\begin{aligned}
 &-\rho^3(2i \sin \theta) + (2i \sin(2\theta)) - \rho^{-3}(2i \sin \theta) \\
 &= -\rho^3(2i \sin \theta) + (2i(2 \sin \theta \cos \theta)) - \rho^{-3}(2i \sin \theta) \\
 &= -2i \sin \theta(\rho^3 + \rho^{-3} - 2 \cos \theta).
 \end{aligned}$$

Tendo isso calculado, voltamos no cálculo do discriminante de η , ou seja,

$$\begin{aligned}
 D(\eta) &= \begin{vmatrix} 1 & \eta & \eta^2 \\ 1 & \rho e^{i\theta} & \rho^2 e^{2i\theta} \\ 1 & \rho e^{-i\theta} & \rho^2 e^{-2i\theta} \end{vmatrix}^2 = (-2i \sin \theta(\rho^3 + \rho^{-3} - 2 \cos \theta))^2 \\
 &= (-2i)^2 \sin^2 \theta(\rho^3 + \rho^{-3} - 2 \cos \theta)^2 = 4 \sin^2 \theta(\rho^3 + \rho^{-3} - 2 \cos \theta)^2.
 \end{aligned}$$

Pelo Lema 4.5.1, segue que

$$\begin{aligned}
 |D(\eta)| &= 4 \cdot \left[\sin^2 \theta \underbrace{(\rho^3 + \rho^{-3})}_{\in \mathbb{R}} - 2 \cos \theta \right]^2 < 4 [(\rho^3 + \rho^{-3})^2 + 4] \\
 &= 4(\rho^6 + 2 \cdot \cancel{(\rho^3 \rho^{-3})}^1 + \rho^{-6} + 4) = 4(\rho^6 + \rho^{-6} + 6) = 4(\eta^3 + \eta^{-3} + 6),
 \end{aligned}$$

e assim,

$$|D(\eta)| < 4(\eta^3 + \eta^{-3} + 6) \quad (4.23)$$

Pela Proposição 2.5.21, se $\mathbb{K}$ é um corpo algébrico de grau n e $\lambda_1, \dots, \lambda_n \in \mathcal{O}_{\mathbb{K}}$ são tais que $D(\lambda_1, \dots, \lambda_n) \neq 0$, então

$$|d(\mathbb{K})| \leq |D(\lambda_1, \dots, \lambda)|.$$

Como $\mathbb{K}$ é corpo cúbico, segue que

$$|d(K)| \leq |D(\alpha, \beta, \gamma)|, \text{ para quaisquer } \alpha, \beta, \gamma \in \mathcal{O}_{\mathbb{K}}, \text{ com } D(\alpha, \beta, \gamma) \neq 0.$$

Assim, em particular, para $1, \eta, \eta^2 \in \mathcal{O}_{\mathbb{K}}$, segue que

$$\begin{aligned} |d(\mathbb{K})| &\leq |D(1, \eta, \eta^2)| = |D(\eta)| \stackrel{(4.23)}{<} 4(\eta^3 + \eta^{-3} + 6) \\ &\Rightarrow |d(\mathbb{K})| < 4(\eta^3 + \eta^{-3} + 6) \Rightarrow \eta^3 + \eta^{-3} > \frac{|d(\mathbb{K})|}{4} - 6. \end{aligned}$$

Note que

$$\begin{aligned} 0 &= \eta^6 - \eta^6 - 1 + 1 = \eta^6 - \eta^3(\eta^3) - \eta^3(\eta^{-3}) + 1 \\ &= \eta^6 - \eta^3(\eta^3 + \eta^{-3}) + 1 \Rightarrow \eta^6 - \eta^3 \left(\frac{|d(\mathbb{K})|}{4} - 6 \right) + 1 > 0. \end{aligned}$$

Completando quadrados, segue que

$$\begin{aligned} &(\eta^3)^2 - 2 \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) \eta^3 + \left(\frac{|d(\mathbb{K})|}{8} - 3 \right)^2 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right)^2 + 1 > 0 \\ &\Rightarrow \left(\eta^3 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) \right)^2 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right)^2 + 1 \\ &\Rightarrow \left(\eta^3 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) \right)^2 > \left(\frac{|d(\mathbb{K})|}{8} - 3 \right)^2 - 1. \end{aligned}$$

Como por hipótese $|d(\mathbb{K})| \geq 33$, segue que podemos aplicar o Lema 4.5.2. Assim,

$$\begin{aligned} &\left(\eta^3 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) \right)^2 > \left(\frac{|d(\mathbb{K})|}{8} - 3 \right)^2 - 1 \\ &\Rightarrow \left| \eta^3 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) \right| > \left| \frac{|d(\mathbb{K})|}{8} - \frac{15}{4} \right| = \frac{|d(\mathbb{K})|}{8} - \frac{15}{4}. \end{aligned}$$

Se $\eta^3 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) < 0$, então $\left(\frac{|d(\mathbb{K})|}{8} - 3 \right) - \eta^3 > \frac{|d(\mathbb{K})|}{8} - \frac{15}{4}$, ou seja,

$$\begin{aligned} &\frac{\cancel{|d(\mathbb{K})|}}{8} - \frac{\cancel{|d(\mathbb{K})|}}{8} - 3 - \eta^3 + \frac{15}{4} > 0 \\ &\Rightarrow -\eta^3 + \frac{3}{4} > 0 \Rightarrow \frac{3}{4} > \eta^3 \\ &\Rightarrow \eta < \sqrt[3]{\frac{3}{4}} \approx 0.9085602964 < 1. \end{aligned}$$

Mas, isso é um absurdo, uma vez que $\eta > 1$. Dessa forma,

$$\eta^3 - \left(\frac{|d(\mathbb{K})|}{8} - 3 \right) \geq 0,$$

ou seja,

$$\eta^3 - \frac{|d(\mathbb{K})|}{8} + 3 > \frac{|d(\mathbb{K})|}{8} - \frac{15}{4} \Rightarrow \eta^3 > \frac{|d(\mathbb{K})|}{8} + \frac{|d(\mathbb{K})|}{8} - 3 - \frac{15}{4} = \frac{|d(\mathbb{K})|}{4} - \frac{27}{4} = \frac{|d(\mathbb{K})| - 27}{4}.$$

Assim,

$$\eta^3 > \frac{|d(\mathbb{K})| - 27}{4},$$

o que prova o teorema. $\square$

A seguir, usamos o Teorema 4.5.3 para determinar a unidade fundamental $\eta > 1$ do anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$.

Teorema 4.5.4. *A unidade fundamental $\eta > 1$ de $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})}$ é $1 + (\sqrt[3]{2}) + (\sqrt[3]{2})^2$.*

Demonstração. Seja $\alpha = \sqrt[3]{2}$ e $\mathbb{K} = \mathbb{Q}(\alpha)$. Pelo Teorema 2.4.10, segue que o anel de inteiros de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2.$$

e o discriminante de $\mathbb{K}$ foi calculado no Exemplo 2.5.18. Assim,

$$d(\mathbb{K}) = -108.$$

Para $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$, segue que $n = 3$, $r = 1$ e $s = 1$. Assim, pelo Teorema 4.3.4 e Corolário 4.4.15, segue que $\mathbb{K}$ possui uma única unidade fundamental $\eta > 1$. Agora, mostramos que

$$\eta = 1 + \alpha + \alpha^2.$$

Para isso, seja $u = 1 + \alpha + \alpha^2 \in \mathcal{O}_{\mathbb{K}}$. Como $\alpha = \sqrt[3]{2}$, segue que $0 < \alpha < 2$. Além disso, $7^3 = 343 < 400 = 20^2$, e assim,

$$1 < u < \underbrace{1 + 2 + 4}_{1 + \alpha + \alpha^2} = 7 < 20^{2/3}.$$

Mais ainda, u é uma unidade de $\mathcal{O}_{\mathbb{K}}$, uma vez que

$$\begin{aligned} u^{-1} &= \frac{1}{u} = \frac{1}{1 + \alpha + \alpha^2} = \frac{1}{(1 + \alpha + \alpha^2)} \cdot \frac{-1 + \alpha}{-1 + \alpha} = \frac{-1 + \alpha}{(1 + \alpha + \alpha^2)} \\ &= \frac{-1 + \alpha}{-1 + \alpha^3} \stackrel{\alpha = \sqrt[3]{2}}{=} \frac{-1 + \alpha}{-1 + 2} = -1 + \alpha \in \mathcal{O}_{\mathbb{K}} \Rightarrow u^{-1} \in \mathcal{O}_{\mathbb{K}}. \end{aligned}$$

Como $|d(\mathbb{K})| = 108 > 33$, pelo Teorema 4.5.3, segue que

$$\eta^3 > \frac{|d(\mathbb{K})| - 27}{4} = \frac{108 - 27}{4} = \frac{81}{4} = 20 \Rightarrow \eta > (20)^{1/3}.$$

Portanto,

$$1 < u < \eta^2. \quad (4.24)$$

Como η é unidade fundamental de $\mathcal{O}_{\mathbb{K}}$ e as únicas raízes da unidade de $\mathcal{O}_{\mathbb{K}}$ são ± 1 (Corolário 4.4.15), pelo *Teorema das Unidades de Dirichlet* segue que

$$u = \pm \eta^k, \text{ para algum } k \in \mathbb{Z}. \quad (4.25)$$

Como $\eta > 1$, segue que

$$u = \eta^k,$$

pela Equação 4.24. Além disso, deduzimos também que $k = 1$, ou seja, $u = \eta$. Portanto, $\eta = 1 + \alpha + \alpha^2 = 1 + (\sqrt[3]{2}) + (\sqrt[3]{2})^2$. $\square$

No próximo teorema determinamos de maneira similar qual a unidade fundamental $\eta > 1$ do anel de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt[3]{3})$.

Teorema 4.5.5. *A unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt[3]{3})}$ é $4 + 3(\sqrt[3]{3}) + 2(\sqrt[3]{3})^2$.*

Demonstração. Considere $\alpha = \sqrt[3]{3}$ e $\mathbb{K} = \mathbb{Q}(\alpha)$. Pelo Teorema 2.4.10, segue que o anel de inteiros de $\mathbb{K}$ é dado por

$$\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}(\alpha) + \mathbb{Z}(\alpha)^2.$$

Além disso, pelo Exemplo 2.5.19,

$$d(\mathbb{K}) = -243.$$

Ainda, para $\mathbb{K} = \mathbb{Q}(\sqrt[3]{3})$, $n = 3$, $r = 1$ e $s = 1$, pelo Teorema 4.3.4 e Corolário 4.4.15, segue que $\mathcal{O}_{\mathbb{K}}$ possui uma única unidade fundamental $\eta > 1$. Mostramos que

$$\eta = 4 + 3\alpha + 2\alpha^2.$$

Seja $u = 4 + 3\alpha + 2\alpha^2 \in \mathcal{O}_{\mathbb{K}}$. Como $\alpha = \sqrt[3]{3}$, segue que $0 < \alpha < \frac{3}{2}$, e assim,

$$0 < u < 4 + 3\left(\frac{3}{2}\right) + 2\left(\frac{3}{2}\right)^2 = 13.$$

Agora, mostramos que u é uma unidade de $\mathcal{O}_{\mathbb{K}}$. Para isso, precisamos encontrar $r, s, t \in \mathbb{Z}$ tais que

$$(4 + 3\alpha + 2\alpha^2)(r + s\alpha + t\alpha^2) = 1.$$

Agora,

$$\begin{aligned} & (4 + 3\alpha + 2\alpha^2)(r + s\alpha + t\alpha^2) \\ &= 4r + 4s\alpha + 4t\alpha^2 + 3r\alpha + 3s\alpha^2 + 3t\alpha^3 + 2r\alpha^2 + 2s\alpha^3 + 2t\alpha^4. \end{aligned} \tag{4.26}$$

Como

$$\alpha^3 = (\sqrt[3]{3})^3 = 3 \text{ e } \alpha^4 = (\sqrt[3]{3})^3(\sqrt[3]{3})^1 = 3\alpha,$$

e substituindo na Equação 4.26, segue que

$$\begin{aligned} & 4r + 4s\alpha + 4t\alpha^2 + 3r\alpha + 3s\alpha^2 + 3t \underbrace{\alpha^3}_3 + 2r\alpha^2 + 2s \underbrace{\alpha^3}_3 + 2t \underbrace{\alpha^4}_{3\alpha} \\ &= 4r + 4s\alpha + 4t\alpha^2 + 3r\alpha + 3s\alpha^2 + 9t + 2r\alpha^2 + 6s + 6t\alpha \\ &= (4r + 6t + 9t) + (3r + 4s + 6t)\alpha + (2r + 3s + 4t)\alpha^2. \end{aligned}$$

Nosso objetivo é encontrar essa expressão igual 1, ou seja,

$$(4r + 6t + 9t) + (3r + 4s + 6t)\alpha + (2r + 3s + 4t)\alpha^2 = 1.$$

Pela igualdade de polinômios, segue que

$$\begin{cases} 4r + 6t + 9t = 1 \\ 3r + 4s + 6t = 0 \\ 2r + 3s + 4t = 0. \end{cases}$$

Resolvendo o sistema linear por matrizes, segue que

$$\begin{bmatrix} 4 & 6 & 9 \\ 3 & 4 & 6 \\ 2 & 3 & 4 \end{bmatrix} \begin{bmatrix} r \\ s \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} 4 & 6 & 9 \\ 0 & -\frac{1}{2} & -\frac{3}{4} \\ 0 & 0 & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} r \\ s \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ -\frac{3}{4} \\ -\frac{1}{2} \end{bmatrix},$$

ou seja,

$$\begin{cases} -\frac{1}{2}t = -\frac{1}{2} \\ -\frac{1}{2}s = \frac{3}{4} - \left(-\frac{3}{4} \cdot 1\right) = 0 \\ 4s = 1 - 6 \cdot 0 - 9 \cdot 1 = -8 \end{cases} \Rightarrow \begin{cases} t = 1 \\ s = 0 \\ r = -2. \end{cases}$$

Dessa forma,

$$r + s\alpha + t\alpha^2 = -2 + 0\alpha + 1\alpha^2 \text{ e } \frac{1}{4 + 3\alpha + 2\alpha^2} = -2 + \alpha^2 \in \mathcal{O}_{\mathbb{K}}.$$

Portanto, $4 + 3\alpha + 2\alpha^2 \in U(\mathcal{O}_{\mathbb{K}})$. Pelo Teorema 4.5.3, segue que

$$\eta^3 > \frac{|d(\mathbb{K})| - 27}{4} = \frac{243 - 27}{4} = 54.$$

Assim,

$$(\eta^3)^2 > (54)^2 \Leftrightarrow \eta^6 > 2916 > 2744 = 14^3 \Rightarrow \eta^2 > 14.$$

Dessa forma, acabamos de mostrar que

$$1 < u < \eta^2.$$

Analogamente a prova do Teorema 4.5.4, deduzimos que $u = \eta$, como queríamos. $\square$

A seguir, apresentamos a Tabela com as unidades fundamentais $\eta > 1$ para alguns corpos cúbicos puros, isto é, $\mathbb{Q}(\sqrt[3]{m})$, com $m \in \mathbb{N}$ que não é um cubo perfeito.

m	Unidade Fundamental $\eta > 1$ de $\mathbb{Q}(\sqrt[3]{m})$
2	$1 + (\sqrt[3]{2}) + (\sqrt[3]{2})^2$
3	$4 + 3(\sqrt[3]{3}) + 2(\sqrt[3]{3})^2$
5	$41 + 24(\sqrt[3]{5}) + 14(\sqrt[3]{5})^2$
6	$109 + 60(\sqrt[3]{6}) + 33(\sqrt[3]{6})^2$
7	$4 + 2(\sqrt[3]{7}) + (\sqrt[3]{7})^2$
11	$89 + 40(\sqrt[3]{11}) + 18(\sqrt[3]{11})^2$
12	$55 + 24(\sqrt[3]{12}) + 21(\sqrt[3]{12})^2/2$

Tabela 4.2: Unidade fundamental em corpos cúbicos puros $\mathbb{Q}(\sqrt[3]{m})$

Alguns valores de Unidade Fundamental se repetem, como nos seguintes corpos

$$\mathbb{Q}(\sqrt[3]{4}) = \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{9}) = \mathbb{Q}(\sqrt[3]{3}), \mathbb{Q}(\sqrt[3]{16}) = \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{18}) = \mathbb{Q}(\sqrt[3]{12}).$$

A seguir, vamos apresentar na Tabela 4.3, a unidade fundamental dos primeiros 30 corpos cúbicos $\mathbb{K}$ com exatamente uma imersão real. Estes corpos estão organizados em ordem crescente pelo valor de seus discriminantes $|d(\mathbb{K})|$, que estão variando entre $-268 \leq d(\mathbb{K}) < 0$. Essas unidades podem ser verificadas de maneira similar aos exemplos anteriores.

$d(\mathbb{K})$	$\mathbb{K} = \mathbb{Q}(\theta)$	Unidade Fundamental
-23	$x^3 + x^2 - 1$	$\theta + \theta^2$
-31	$x^3 - x^2 - 1$	θ
-44	$x^3 - x^2 - x - 1$	θ
-59	$x^3 + 2x - 1$	$2 + \theta^2$
-76	$x^3 - 2x - 2$	$1 + \theta$
-83	$x^3 - x^2 + x - 2$	$1 + \theta$
-87	$x^3 + x^2 + 2x - 1$	$2 + \theta + \theta^2$
-104	$x^3 - x - 2$	$1 + \theta + \theta^2$
-107	$x^3 - x^2 + 3x - 2$	$3 + \theta^2$
-108	$x^3 - 2$	$1 + \theta + \theta^2$
-116	$x^3 - x^2 - 2$	$1 + \theta + \theta^2$
-135	$x^3 - 3x - 1$	$3 + \theta^2$
-139	$x^3 + x^2 + x - 2$	$3 + 2\theta + \theta^2$
-140	$x^3 + 2x - 2$	$3 + \theta + \theta^2$
-152	$x^3 - x^2 + 2x - 2$	$1 + \theta + \theta^2$
-172	$x^3 + x^2 - x - 3$	$2 + 2\theta + \theta^2$
-175	$x^3 - x^2 + 2x - 3$	$2 + \theta^2$
-199	$x^3 - x^2 + 4x - 1$	$4 - \theta + \theta^2$
-200	$x^3 + x^2 + 2x - 2$	$9 + 5\theta + 3\theta^2$
-204	$x^3 - x^2 + x - 3$	$4 + \theta + 2\theta^2$
-211	$x^3 - 2x - 3$	$2 + 2\theta + \theta^2$
-212	$x^3 - x^2 + 4x - 2$	$15 - 2\theta + 4\theta^2$
-216	$x^3 - 3x - 2$	$17 + 3\theta + 5\theta^2$
-231	$x^3 + x^2 - 3$	$2 + 2\theta + \theta^2$
-239	$x^3 - x - 3$	$2 + 2\theta + \theta^2$
-243	$x^3 - 3$	$4 + 3\theta + 2\theta^2$
-244	$x^3 + x^2 - 4x - 6$	$5 + 6\theta + 2\theta^2$
-247	$x^3 + x - 3$	$2 + \theta + \theta^2$
-255	$x^3 - x^2 - 3$	$2 + \theta + \theta^2$
-268	$x^3 + x^2 - 3x - 5$	$3 + 3\theta + \theta^2$

Tabela 4.3: Unidade fundamental de corpos cúbicos com apenas uma imersão real

Até agora analisamos as unidades de corpos cúbicos com apenas uma imersão real. Já vimos que nesse caso, a unidade fundamental é única. Por outro lado, em corpos cúbicos com três imersões reais (corpos totalmente reais), obtemos um sistema de unidades fundamentais $\{\epsilon_1, \epsilon_2\}$ de $\mathcal{O}_{\mathbb{K}}$.

Para vermos um exemplo de como podemos determinar o sistema de unidades fundamentais para $\mathcal{O}_{\mathbb{K}}$, $\mathbb{K} = \mathbb{Q}(\theta) \in \mathbb{R}$, usamos o auxílio de uma tabela que contém o

sistema de unidades fundamentais para os primeiros trinta corpos cúbicos $\mathbb{K} = \mathbb{Q}(\theta) \in \mathbb{R}$, organizados em ordem crescente pelos seus discriminantes $|d(\mathbb{K})|$.

$d(\mathbb{K})$	$\mathbb{K} = \mathbb{Q}(\theta)$	ϵ_1	ϵ_2
49	$x^3 + x^2 - 2x - 1$	$-1 + \theta + \theta^2$	$2 - \theta^2$
81	$x^3 - 3x - 1$	$2 + \theta - \theta^2$	$-\theta$
148	$x^3 + x^2 - 3x - 1$	θ	$2 - \theta^2$
169	$x^3 - x^2 - 4x - 1$	$2 + 2\theta - \theta^2$	$-\theta$
229	$x^3 - 4x - 1$	θ	$2 + \theta$
257	$x^3 - 5x - 3$	$4 + \theta - \theta^2$	$5 + \theta - \theta^2$
316	$x^3 + x^2 - 4x - 2$	$-3 + \theta + \theta^2$	$-5 + \theta + \theta^2$
321	$x^3 + x^2 - 4x - 1$	$-\theta$	$-1 + 2\theta + \theta^2$
361	$x^3 + x^2 - 6x - 7$	$4 + \theta - \theta^2$	$5 - \theta^2$
404	$x^3 - x^2 - 5x - 1$	$-\theta$	$1 - \theta - \theta^2$
469	$x^3 + x^2 - 5x - 4$	$-1 - \theta$	$-1 + 2\theta + \theta^2$
473	$x^3 - 5x$	$-1 - \theta$	$-2 - \theta$
564	$x^3 + x^2 - 5x - 3$	$-2 + \theta$	$-1 - \theta + \theta^2$
568	$x^3 - x^2 - 6x - 2$	$-5 - \theta + \theta^2$	$-7 - 4\theta + 2\theta^2$
621	$x^3 - 6x - 3$	$-2 - \theta$	$1 + 2\theta$
697	$x^3 - x^2 - 8x - 5$	$6 + 2\theta - \theta^2$	$7 + 2\theta - \theta^2$
733	$x^3 + x^2 - 7x - 8$	$1 + \theta$	$-5 - 2\theta$
756	$x^3 - 6x - 2$	$5 - \theta^2$	$11 + \theta - 2\theta^2$
761	$x^3 - x^2 - 6x - 1$	θ	$2 + \theta$
785	$x^3 + x^2 - 6x - 5$	$1 + \theta$	$-4 + \theta + \theta^2$
788	$x^3 - x^2 - 7x - 3$	$2 + \theta$	$-1 - 2\theta$
837	$x^3 - 6x - 1$	$-\theta$	$-3 - 6\theta - 2\theta^2$
892	$x^3 + x^2 - 8x - 10$	$3 + \theta - \theta^2$	$1 + 3\theta + \theta^2$
940	$x^3 - 7x - 4$	$-11 - 2\theta + 2\theta^2$	$-3 + \theta + \theta^2$
961	$x^3 + x^2 - 10x - 8$	$-1 + 2\theta + 2\theta^2$	$3 + 4\theta - 2\theta^2$
985	$x^3 + x^2 - 6x - 1$	θ	$-2 + \theta$
993	$x^3 + x^2 - 6x - 3$	$5 - \theta - \theta^2$	$5 - \theta^2$
1016	$x^3 + x^2 - 6x - 2$	$7 - \theta - \theta^2$	$-11 - \theta + \theta^2$
1076	$x^3 - 8x - 6$	$1 + \theta$	$-7 - 3\theta$
1101	$x^3 + x^2 - 9x - 12$	$5 + 2\theta - \theta^2$	$-7 - 4\theta + 2\theta^2$

Tabela 4.4: Sistema de unidades fundamentais de corpos cúbicos totalmente reais

Exemplo 4.5.6. Considere o polinômio $q(x) = x^3 - 4x + 2 \in \mathbb{Z}[x]$. Observe que $q(x)$ é irreduzível sobre $\mathbb{Z}$ pelo critério de Eisenstein para o primo $p = 2$. Dessa forma, $\mathbb{K} = \mathbb{Q}(\theta)$, onde $\theta^3 - 4\theta + 2 = 0$, é um corpo cúbico. O discriminante de $q(x) = x^3 - 4x + 2$ é dado por

$$-4(-4)^3 - 2 + (2)^2 = 148 = 2^2 \cdot 37,$$

ou seja, $\mathbb{K}$ tem três imersões reais uma vez que, $D(p) > 0$. Mais ainda, pela fatoração do discriminante do polinômio, obtemos duas possibilidades para o discriminante do corpo,

$$d(\mathbb{K}) = 148 \text{ ou } 37.$$

Mas, pela Tabela 4.4, o menor discriminante de um corpo cúbico com três imersões reais é 49. Portanto, $d(\mathbb{K}) > 49 \Rightarrow d(\mathbb{K}) = 148$. Logo, $\mathbb{K}$ deve ser o terceiro corpo listado, isto é,

$$\mathbb{K} = \mathbb{Q}(\phi), \text{ com } \phi^3 + \phi^2 - 3\phi - 1 = 0.$$

Note que podemos relacionar θ com ϕ através da relação

$$\phi = \frac{1}{(\theta - 1)},$$

uma vez que se ϕ é raiz de $f(x) = x^3 + x^2 - 3x - 1$ e θ é raiz de $g(x) = x^3 - 4x + 2$, então $\phi = \frac{1}{\theta - 1}$ é raiz de $f(x)$, uma vez que

$$\begin{aligned} f\left(\frac{1}{\theta - 1}\right) &= \left(\frac{1}{\theta - 1}\right)^3 + \left(\frac{1}{\theta - 1}\right)^2 - 3\left(\frac{1}{\theta - 1}\right) - 1 \\ &= \frac{1}{(\theta - 1)^3} + \frac{1}{(\theta - 1)^2} - 3 \cdot \frac{1}{(\theta - 1)} - 1 \\ &= \frac{1 + (\theta - 1) - 3(\theta - 1)^2 - (\theta - 1)^3}{(\theta - 1)^3} \\ &= \frac{1 + \theta - 1 - 3\theta^2 + 6\theta - 3 - \theta^3 + 3\theta^2 - 3\theta + 1}{(\theta - 1)^3} \\ &= \frac{-\theta^3 + 4\theta - 2}{(\theta - 1)^3} = 0 \end{aligned}$$

se, e somente se,

$$-\theta^3 + 4\theta - 2 = 0 \Leftrightarrow -(\theta^3 - 4\theta + 2) = -g(\theta) = 0.$$

Portanto, $f\left(\frac{1}{\theta - 1}\right) = 0$. Pela Tabela 4.4, um sistema de unidades fundamentais para $\mathcal{O}_{\mathbb{K}}$ é

$$\{\phi, 2 - \phi^2\}.$$

Agora, vamos encontrar qual o sistema fundamental em termos de θ . Observe que

$$\phi = \frac{1}{\theta} \Leftrightarrow \phi \cdot \theta = 1 = (\theta - 1)^0$$

e

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

Assim, $(2 - \phi^2)(2\theta^2 - 4\theta + 1) = (\theta - 1)^2$. Portanto, um sistema de unidades fundamental em termos de θ pode ser dado por

$$\{\theta - 1, 2\theta^2 - 4\theta + 1\}.$$

Mais ainda, como

$$(2\theta - 1)(2\theta^2 - 4\theta + 1) = 4\theta^3 - 10\theta^2 + 6\theta - 1 = \theta(\theta^3 - 4\theta + 2) - (\theta^4 - 4\theta^3 + 6\theta^2 - 4\theta + 1) = -(\theta - 1)^4,$$

segue que podemos simplificar e apresentar o seguinte sistema de unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$,

$$\{\theta - 1, 2\theta - 1\}.$$

Por fim, apesar de não ser o foco desta seção, vamos apresentar uma tabela que fornece uma unidade fundamental para alguns corpos quárticos puros $\mathbb{Q}(\sqrt[4]{-m})$, com $m \in \mathbb{N}$, onde esses corpos de grau 4 são totalmente imaginários.

m	Unidade Fundamental de $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt[4]{-m})$
1	$\theta - \theta^2 + \theta^3$
2	$-1 + \theta^2 - \theta^3$
5	$-2 + 2\theta - \theta^2$
6	$1 + 4\theta - 4\theta^2 + 2\theta^3$
10	$-27 + 12\theta - \theta^2 - 3\theta^3$

Tabela 4.5: Unidade fundamental de alguns corpos quárticos puros

As Tabelas 4.2, 4.3, 4.4 e 4.5 foram retiradas da referência [8]. Para calculá-las foi utilizado a referência [25]. Este livro descreve 148 algoritmos que são fundamentais para Teoria dos Números computacional. Os algoritmos 4.9.9 e 4.9.10 que calcularam as raízes da unidade no anel de inteiros. O algoritmo 6.5.8 que calculou o sistema de unidades fundamentais.

4.6 Regulador

Considere $\{\epsilon_1, \dots, \epsilon_{r+s-1}\}$ e $\{\epsilon'_1, \dots, \epsilon'_{r+s-1}\}$ dois sistemas de unidades fundamentais para o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo algébrico $\mathbb{K}$. Como $\{\epsilon_1, \dots, \epsilon_{r+s-1}\}$ é um sistema de unidades fundamental, segue que

$$\epsilon'_j = \zeta^{b_j} (\epsilon_1^{a_{1j}} \dots \epsilon_{r+s-1}^{a_{(r+s-1)j}}), \quad \text{onde } j = 1, 2, \dots, r+s-1, \quad (4.27)$$

onde ζ é uma raiz da unidade em $\mathbb{K}$ e $a_{ij}, b_j \in \mathbb{Z}$. De modo análogo, $\{\epsilon'_1, \dots, \epsilon'_{r+s-1}\}$ é sistema fundamental de unidades. Assim,

$$\epsilon_j = \xi^{b'_j} (\epsilon'_1{}^{a'_{1j}} \dots \epsilon'_{r+s-1}{}^{a'_{(r+s-1)j}}), \quad \text{onde } j = 1, 2, \dots, r+s-1, \quad (4.28)$$

com ξ raiz da unidade em $\mathbb{K}$ e $a'_{ij}, b'_j \in \mathbb{Z}$. Dessa forma, para $j = 1, \dots, r+s-1$, pelas Equações (4.27) e (4.28), segue que

$$\begin{aligned} \epsilon'_j &= \zeta^{b_j} \prod_{k=1}^{r+s-1} \epsilon_k^{a_{kj}} = \zeta^{b_j} \prod_{k=1}^{r+s-1} \left(\xi^{b'_k} \prod_{l=1}^{r+s-1} \epsilon'_l{}^{a'_{lk}} \right)^{a_{kj}} \\ &= (\zeta)^{(b_j + \sum_{k=1}^{r+s-1} a_{kj} b'_k)} \prod_{l=1}^{r+s-1} (\epsilon'_l)^{(\sum_{k=1}^{r+s-1} a'_{lk} a_{kj})} \end{aligned}$$

Pela unicidade da representação de cada unidade, segue que

$$\sum_{k=1}^{r+s-1} a'_{lk} a_{kj} = \begin{cases} 1, & \text{se } l = j; \\ 0, & \text{se } l \neq j. \end{cases} \quad (4.29)$$

Agora, definimos duas matrizes, A e A' , ambas $(r+s-1) \times (r+s-1)$, dadas por

$$A = [a_{ij}] \text{ e } A' = [a'_{ij}]$$

Pela Equação (4.29), segue que

$$A'.A = (Id)_{r+s-1}$$

Dessa forma,

$$\det(A').\det(A) = \det(A'A) = \det(Id_{r+s-1}) = 1.$$

Como as matrizes A e A' são formadas pelos a_{ij} e a'_{ij} , potências das unidades fundamentais, segue que todas suas entradas são inteiras. Logo, $\det(A)$ e $\det(A')$ são valores inteiros. Ainda, como o produto

$$\underbrace{\det(A)}_{\in \mathbb{Z}} \cdot \underbrace{\det(A')}_{\in \mathbb{Z}} = 1,$$

segue que

$$\det(A) = \det(A') = \pm 1.$$

Portanto,

$$|\det(A)| = |\det(A')| = 1. \quad (4.30)$$

Agora, sejam σ_k , onde $k = 1, \dots, n$, os $n = [\mathbb{K} : \mathbb{Q}]$ monomorfismos distintos $\mathbb{K} \rightarrow \mathbb{C}$ com $\sigma_1, \dots, \sigma_r \in \mathbb{R}$ e $\sigma_{r+1}, \dots, \sigma_{r+s} \in \mathbb{C}$ e

$$\begin{cases} \sigma_{r+s-1} = \overline{\sigma_{r+1}} \\ \vdots \\ \sigma_n = \sigma_{r+2s} = \overline{\sigma_{r+s}}. \end{cases}$$

Para $j, k = 1, 2, \dots, r+s-1$, segue que

$$\begin{aligned} \sigma_k(\epsilon'_j) &= \sigma \left(\zeta^{b_j} \prod_{l=1}^{r+s-1} \epsilon_l^{a_{lj}} \right) = \sigma_k(\zeta)^{b_j} \prod_{l=1}^{r+s-1} \sigma_k(\epsilon_l)^{a_{lj}} \Rightarrow \\ |\sigma_k(\epsilon'_j)| &= \left| \sigma_k(\zeta^{b_j}) \prod_{l=1}^{r+s-1} \sigma_k(\epsilon_l)^{a_{lj}} \right| = \underbrace{|\sigma_k(\zeta)|^{b_j}}_1 \cdot \left| \prod_{l=1}^{r+s-1} \sigma_k(\epsilon_l)^{a_{lj}} \right| = \prod_{l=1}^{r+s-1} |\sigma_k(\epsilon_l)|^{a_{lj}} \end{aligned}$$

Aplicando a função logarítmica, segue que

$$\log |\sigma_k(\epsilon'_j)| = \sum_{l=1}^{r+s-1} |\sigma_k(\epsilon_l)|^{a_{lj}} = \sum_{l=1}^{r+s-1} \log |\sigma_k(\epsilon_l)|. \quad (4.31)$$

Agora, sejam E e E' as matrizes $(r+s-1) \times (r+s-1)$ dadas por

$$E = [\log |\sigma_i(\epsilon_j)|] \text{ e } E' = [\log |\sigma_i(\epsilon'_j)|]$$

Assim, pela Equação (4.31), segue que $E = A.E'$, isto é,

$$\begin{aligned} & \begin{bmatrix} \log |\sigma_1(\epsilon_1)| & \dots & \log |\sigma_1(\epsilon_{r+s-1})| \\ \vdots & \ddots & \vdots \\ \log |\sigma_{r+s-1}(\epsilon_1)| & \dots & \log |\sigma_{r+s-1}(\epsilon_{r+s-1})| \end{bmatrix} = \\ & = \begin{bmatrix} a_{11} & \dots & a_{1(r+s-1)} \\ \vdots & \ddots & \vdots \\ a_{(r+s-1)1} & \dots & a_{(r+s-1)(r+s-1)} \end{bmatrix} \cdot \begin{bmatrix} \log |\sigma_1(\epsilon'_1)| & \dots & \log |\sigma_1(\epsilon'_{r+s-1})| \\ \log |\sigma_2(\epsilon'_1)| & \dots & \log |\sigma_2(\epsilon'_{r+s-1})| \\ \vdots & \ddots & \vdots \\ \log |\sigma_{r+s-1}(\epsilon'_1)| & \dots & \log |\sigma_{r+s-1}(\epsilon'_{r+s-1})| \end{bmatrix}. \end{aligned}$$

Assim,

$$\det(E') = \det(AE) = \det(A) \cdot \det(E).$$

Finalmente,

$$\begin{aligned} |\det(E')| &= |\det(A) \cdot \det(E)| = \underbrace{|\det(A)|}_1 |\det(E)| \stackrel{(4.30)}{=} |\det(E)| \Rightarrow \\ |\det(E')| &= |\det(E)| \Leftrightarrow |\det(\log(\sigma_i(\epsilon'_j)))| = |\det(\log(\sigma_i(\epsilon_j)))|. \end{aligned}$$

Com isso, observamos que independente da escolha do sistema de unidades fundamentais $\{\epsilon_1, \dots, \epsilon_{r+s-1}\}$ de $\mathcal{O}_{\mathbb{K}}$, o valor do número real não negativo

$$|\det(\log(\sigma_i(\epsilon_j)))|$$

não se altera. Dessa forma, podemos introduzir o seguinte conceito.

Definição 4.6.1. Seja $\{\epsilon_1, \dots, \epsilon_{r+s-1}\}$ um sistema de unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$. Denote por E a matriz $(r+s-1) \times (r+s-1)$ cujas (i, j) são dadas por $\log |\sigma_i(\epsilon_j)|$, onde $i, j = 1, 2, \dots, r+s-1$. O número real não negativo

$$R(\mathbb{K}) = |\det(E)|$$

é chamado **regulador** de $\mathbb{K}$.

Observação 4.6.2. Na Definição 4.6.1, estamos considerando o logaritmo na base 10. Entretanto, em diversas bibliografias, inclusive em [8] que foi baseada essa seção, é utilizado o logaritmo na base e .

Observação 4.6.3. Se $\mathbb{K}$ é $\mathbb{Q}(\sqrt{-m})$, com m um inteiro positivo, então $\mathbb{K}$ é um corpo quadrático imaginário. Desta forma, $r+s-1 = 0$ e o conjunto do sistemas de unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$ é vazio. Neste caso, consideramos que $R(\mathbb{K})$ é zero. Caso contrário, $R(\mathbb{K}) > 0$.

Vamos determinar agora o regulador de um corpo quadrático real.

Teorema 4.6.4. Se $\mathbb{K}$ é um corpo quadrático real, então

$$R(\mathbb{K}) = \log(\eta),$$

onde η é a unidade fundamental maior do que 1 de $\mathbb{K}$.

Demonstração. Se $\mathbb{K}$ é um corpo quadrático real, então $n = r = 2$ e $s = 0$. Logo, $r + s - 1 = 1$. Portanto, o sistema de unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$ é igual a $\{\eta\}$. Dessa forma,

$$R(\mathbb{K}) = |\det(\log(|\eta|))| = |\log(|\eta|)| \stackrel{\eta > 1}{=} |\log(\eta)| = \log(\eta).$$

Como $\eta > 1$, segue que $\log \eta > 0$. Logo, a função está bem definida. $\square$

Exemplo 4.6.5. Considere o corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{2})$. O sistema de unidades fundamentais de $\mathcal{O}_{\mathbb{K}}$ é dado $\eta = 1 + \sqrt{2}$. Assim,

$$R(\mathbb{K}) = \log(1 + \sqrt{2}).$$

Exemplo 4.6.6. Seja $\mathbb{K}$ o corpo cúbico dado por $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta^3 - 4\theta + 2 = 0$. O discriminante do polinômio $x^3 - 4x + 2$ é positivo, ou seja,

$$-4(-4)^3 - 27(2)^2 = 148 > 0.$$

Dessa forma, as três raízes de $p(x) = x^3 - 4x + 2$, θ, θ' e θ'' , são reais. Logo, $n = r = 3$, $s = 0$ e $r + s - 1 = 2$. Portanto, o sistema de unidades fundamentais contém duas unidades como foi mostrado no Exemplo 4.5.6. Assim, podemos considerar as seguintes unidades fundamentais

$$\theta - 1 \text{ e } 2\theta - 1.$$

Reorganizemos as raízes θ, θ' e θ'' de $x^3 - 4x + 2 = 0$ de modo que

$$\theta < \theta' < \theta''.$$

Calculando o valor das raízes, segue que

$$\theta \approx -2.2143, \theta' = 0.5391 \text{ e } \theta'' = 1.6751.$$

Assim,

$$\begin{aligned} |\theta - 1| &\approx 3.2143 &\Rightarrow \log(3.2143) &\approx 0.5071 \\ |2\theta - 1| &\approx 5.4286 &\Rightarrow \log(5.4286) &\approx 0.7347 \\ |\theta' - 1| &\approx 0.4609 &\Rightarrow \log(0.4609) &\approx -0.3364 \\ |2\theta' - 1| &\approx 0.0782 &\Rightarrow \log(0.0782) &\approx -1.1068 \\ |\theta'' - 1| &\approx 0.6751 &\Rightarrow \log(0.6751) &\approx -0.1706 \\ |2\theta'' - 1| &\approx 2.3502 &\Rightarrow \log(2.3502) &\approx 0.3711 \end{aligned}$$

Agora, calculamos o regulador, ou seja,

$$\begin{aligned} R(\mathbb{K}) &= \left| \det \begin{bmatrix} \log |\theta - 1| & \log |\theta' - 1| \\ \log |2\theta - 1| & \log |2\theta' - 1| \end{bmatrix} \right| \\ &= \left| \det \begin{bmatrix} 0.5071 & -0.3364 \\ 0.7347 & -1.1068 \end{bmatrix} \right| \\ &= |(0.5071)(-1.1068) - (-0.3364)(0.7347)| \\ &= 0.3141 \end{aligned}$$

Também,

$$\begin{aligned}
 R(\mathbb{K}) &= \left| \det \begin{bmatrix} \log |\theta - 1| & \log |\theta'' - 1| \\ \log |2\theta - 1| & \log |2\theta'' - 1| \end{bmatrix} \right| \\
 &= \left| \det \begin{bmatrix} 0.5071 & -0.1706 \\ 0.7347 & 0.3711 \end{bmatrix} \right| \\
 &= |(0.5071)(0.3711) - (-0.1706)(0.7347)| \\
 &= 0.3135
 \end{aligned}$$

e

$$\begin{aligned}
 R(\mathbb{K}) &= \left| \det \begin{bmatrix} \log |\theta'1| & \log |\theta'' - 1| \\ \log |2\theta' - 1| & \log |2\theta'' - 1| \end{bmatrix} \right| \\
 &= \left| \det \begin{bmatrix} -0.3364 & -0.1706 \\ -1.1068 & 0.3711 \end{bmatrix} \right| \\
 &= |(-0.3364)(0.3711) - (-0.1706)(-1.1068)| \\
 &= 0.3137
 \end{aligned}$$

Note que os valores são suficientemente próximos e a diferença vêm da aproximação utilizadas nas raízes e no calculo do log.

5 Unidades em corpos ciclotômicos

Determinar o grupo de unidades de um corpo de números é, em geral, uma tarefa extremamente trabalhosa. No entanto, para corpos ciclotômicos é possível determinar explicitamente tal grupo de unidades, chamadas de unidades ciclotômicas, e que tem índice finito no grupo de todas as unidades.

No presente capítulo, apresentamos as unidades em corpos ciclotômicos, onde as principais bibliografias utilizadas são [13], [14] e [15]. Na Seção 5.1, apresentamos uma breve introdução sobre raízes da unidade e corpos ciclotômicos. Na Seção 5.2, apresentamos o anel de inteiros de um corpo ciclotômico $\mathbb{Q}(\zeta_n)$ em três casos: $n = p$ primo, $n = p^r$ uma potência de primo e, por fim, para n um inteiro positivo qualquer. Na Seção 5.3, apresentamos resultados sobre unidades em corpos ciclotômicos. Finalmente, na Seção 5.4, aprofundamos nas unidades ciclotômicas, que permitem uma categorização mais a fundo do grupo de unidades de $\mathbb{Q}(\zeta_n)$.

5.1 Corpos ciclotômicos

A seguir, apresentamos as raízes da unidade e juntamente com suas principais propriedades e resultados. Estes conceitos são importantes para entender os Corpos Ciclotômicos.

Definição 5.1.1. Seja $\mathbb{K}$ um corpo algébrico.

1. Um elemento $\zeta \in \mathbb{K}$ é chamado de **raiz n -ésima da unidade** se $\zeta^n = 1$, ou seja, se ζ é raiz do polinômio $x^n - 1$, $n \in \mathbb{N}$.
2. Se $\zeta^n = 1$ e $\zeta^m \neq 1$, para todo m tal que $1 \leq m \leq n - 1$, então o elemento ζ é dito **raiz n -ésima primitiva da unidade**.

Por definição, segue que as raízes n -ésimas da unidade são as raízes do polinômio $x^n - 1$. Denotamos por W_n , ou simplesmente por W , o grupo das raízes de $x^n - 1$ dado por $\{\zeta_1, \zeta_2, \dots, \zeta_n\}$.

Uma potência de ζ , digamos ζ^m , é raiz n -ésima primitiva da unidade se, e só se, $\text{mdc}(m, n) = 1$, $m = 1, \dots, n - 1$. Logo, podemos concluir disso que a quantidade de raízes primitivas da unidade é dada pela função φ de Euler, uma vez que, pela Definição 4.4.1,

$$\varphi(n) = \#\{1 \leq m \leq n - 1 : \text{mdc}(m, n) = 1, m, n \in \mathbb{N}\}.$$

Observação 5.1.2. Note que se $\mathbb{K}$ tem característica p e $x \in W$, então sua ordem n não é um múltiplo de p .

A seguir, vamos apresentar alguns resultados que são úteis no estudo das unidades de corpos ciclotômicos, que serão apresentados ainda neste capítulo.

Teorema 5.1.3. *Seja c um número real positivo. Se $\mathbb{K}$ é um corpo de números, então existe apenas uma quantidade finita de inteiros algébricos x em $\mathbb{K}$ tal que $|x^{(i)}| \leq c$, para todos os conjugados $x^{(i)}$ de x .*

Demonstração. Vamos primeiramente determinar um conjunto finito S que dependa somente de c . Seja $[\mathbb{K} : \mathbb{Q}] = n$ e seja $s_1, s_2, s_3, \dots, s_n$ os polinômios simétricos elementares em n variáveis, dadas por

$$\begin{aligned} s_1 &= X_1 + X_2 + \dots + X_N \\ s_2 &= \sum_{i < j} X_i X_j \\ &\vdots \\ s_n &= X_1 X_2 \dots X_N \end{aligned}$$

Seja c' um número real suficientemente grande, por exemplo, considere

$$c' = \max \left\{ nc, \binom{n}{2} c^2, \dots, \binom{n}{k} c^k, \dots, c^n \right\}.$$

Queremos mostrar que se x é um inteiro algébrico de $\mathbb{K}$ tal que $|x^{(i)}| \leq c$, para todos seus conjugados $x^{(i)}$, então $x \in S$. Seja F o conjunto de todos polinômios mônicos de grau no máximo n , cujos coeficientes são inteiros a que satisfazem $|a| \leq c'$. Note que F é um conjunto finito. Finalmente, defina S sendo o conjunto dos elementos de $\mathbb{K}$ que são raiz de algum polinômio pertencente a F . Como F é finito, segue que S também é finito. Assim, se

$$|x^{(i)}| \leq c, \text{ para todos conjugados de } x \in \mathbb{K},$$

então

$$|s_k(x^{(1)}, x^{(2)}, \dots, x^{(n)})| \leq c', \text{ para todo } k = 1, \dots, n.$$

Como x é um inteiro algébrico por hipótese, segue que $s_k((x^{(1)}, x^{(2)}, \dots, x^{(n)})) \in \mathbb{Z}$ e, portanto, o polinômio $\prod_{i=1}^n (X - x^{(i)}) \in F$, ou seja, $x \in S$. De S ser finito, segue que existe apenas uma quantidade finita de inteiros algébricos $x \in \mathbb{K}$ que satisfazem $|x^{(i)}| \leq c$, para todos os conjugados $x^{(i)}$ de x . $\square$

O próximo corolário, segue do Teorema 5.1.3 e fornece uma caracterização das raízes da unidade de $\mathbb{K}$.

Corolário 5.1.4. *O elemento x é uma raiz da unidade em $\mathbb{K}$ se, e somente se, x é um inteiro algébrico de $\mathbb{K}$ tal que $|x^{(i)}| = 1$, para todo conjugado $x^{(i)}$ de x .*

Demonstração. Se x é uma raiz da unidade, o mesmo vale para seus conjugados. Por definição, segue que

$$x^m = 1 \Rightarrow |x|^m = 1 \Rightarrow |x| = 1.$$

O mesmo vale para qualquer conjugado de x . Assim, obtemos o que queríamos. Reciprocamente, pelo Teorema 5.1.3, segue que existe um número finito de inteiros algébricos $x \in \mathbb{K}$ tal que

$$|x^{(i)}| = 1, \text{ para todos os conjugados de } x.$$

As potências $x, x^2, x^3, \dots$, satisfazem a mesma propriedade. Assim, existe inteiros r e s , com $r < s$, tais que

$$x^r = x^s \Rightarrow x^{s-r} = 1,$$

ou seja, x é uma raiz da unidade. $\square$

O próximo teorema é uma junção dos Teoremas 5.1.3 e 5.1.4, e fornece informações sobre a estrutura do grupo W

Teorema 5.1.5. *O grupo W das raízes da unidade em $\mathbb{K}$ é um grupo multiplicativo cíclico.*

Demonstração. Segue direto dos Teoremas 5.1.3 e 5.1.4 que W deve ser finito. Assim, considere h a ordem máxima dos elementos de W . Pela Teoria de Grupos, segue que a ordem de todos os elementos de W devem dividir h . Logo, W está contido no grupo das h -ésimas raízes da unidade, que por sua vez é um grupo cíclico. Portanto, W é cíclico. $\square$

Observação 5.1.6. Segue diretamente que os geradores de W são as potências de ζ_n .

Agora, considere $\mathbb{K}$ um corpo algebricamente fechado. Seja $n \in \mathbb{N}$ tal que $(n, p) = 1$, onde p é a característica de $\mathbb{K}$. Desse modo, $x^n - 1$ tem exatamente n raízes distintas em $\mathbb{K}$, que por definição são elementos de W .

Observação 5.1.7. Para $\mathbb{K} = \mathbb{Q}$, o número complexo

$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$$

é uma raiz n -ésima primitiva da unidade e suas potências $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$ são distintas e dividem a circunferência de raio 1 em n partes iguais.

Da Observação 5.1.7, podemos definir o conceito de polinômio ciclotômico.

Definição 5.1.8. O polinômio $\phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^n (x - \zeta_n^j)$ é chamado de **n -ésimo polinômio ciclotômico** e seu grau é $\varphi(n)$.

Exemplo 5.1.9. Se p é primo, então $x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \dots + x + 1)$, onde $\phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ é irredutível sobre $\mathbb{Q}$. Além disso, $\phi_p(x)$ é o polinômio minimal de ζ_p e suas raízes são $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$, que são raízes p -ésimas da unidade.

Dando seguimento, obtemos os seguintes resultados envolvendo o polinômio ciclotômico.

Proposição 5.1.10. *Se n é um inteiro positivo, então $x^n - 1 = \prod_{d|n} \phi_d(x)$.*

Demonstração. As raízes de $f(x) = x^n - 1$ são dadas por $1, \zeta, \zeta^2, \dots, \zeta^{n-1}$. Assim,

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \dots (x - \zeta^{n-1}).$$

Observe que W_d é um subgrupo de W_n para todo d que divide n . Analisando as ordens de cada raiz de $f(x)$ e escrevendo todas as raízes de mesma ordem como um polinômio da forma $\phi_d(x) = \prod_{\text{período } \zeta=d} (x - \zeta)$, segue que $x^n - 1 = \prod_{d|n} \phi_d(x)$, o que prova a proposição. $\square$

Como uma consequência imediata, obtemos o seguinte corolário.

Corolário 5.1.11. *Se n é um inteiro positivo, então*

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

Observação 5.1.12. Quando $n = p$, p primo, o p -ésimo polinômio ciclotômico é dado por

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1.$$

Este acima é o polinômio minimal de ζ sobre $\mathbb{Q}$, o que já implica que ζ pertence ao anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta)$. Em particular, para $x = 1$,

$$\phi_p(1) = \prod_{i=1}^{p-1} (1 - \zeta^i) = p.$$

Essa relação pode ser expandida para potências de p da seguinte forma:

$$\phi_p^r(x) = x^{p^{r-1}(p-1)} + x^{p^{r-2}(p-2)} + \dots + x^{p^{r-1}} + 1.$$

Observação 5.1.13. Outro fato a se observar é que os elementos $1 - \zeta, 1 - \zeta^2, \dots, 1 - \zeta^{p-1}$ são associados.

Definição 5.1.14. Um **corpo ciclotômico** $\mathbb{Q}(\zeta)$ é um corpo gerado por uma raiz n -ésima da unidade sobre um corpo $\mathbb{K}$.

Observação 5.1.15. Um n -ésimo corpo ciclotômico é a menor extensão de $\mathbb{Q}$ que contém as raízes do polinômio $x^n - 1$, com $n \in \mathbb{N}$, $n \geq 2$.

Ainda, lembre que da Teoria de Galois, sabemos que

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Isso segue do fato que $\phi_n(x) \in \mathbb{Z}[x]$ e é irredutível sobre $\mathbb{Q}$ quando ζ_n é uma raiz n -ésima primitiva da unidade.

Observação 5.1.16. Pela definição de ζ_n , segue que

$$\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right) \Rightarrow \zeta_n^{-1} = \cos\left(\frac{2\pi}{n}\right) - i \operatorname{sen}\left(\frac{2\pi}{n}\right).$$

Assim,

$$\zeta_n + \zeta_n^{-1} = \cos\left(\frac{2\pi}{n}\right) + i \operatorname{sen}\left(\frac{2\pi}{n}\right) + \cos\left(\frac{2\pi}{n}\right) - i \operatorname{sen}\left(\frac{2\pi}{n}\right) = 2 \cos\left(\frac{2\pi}{n}\right),$$

que é um número real. Portanto,

$$\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{R}.$$

Proposição 5.1.17. *Se ζ_n é uma raiz n -ésima primitiva da unidade, então*

$$[\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2},$$

onde φ é a função de Euler.

Demonstração. Como $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n)$, pelo Teorema da Multiplicidade dos Graus 2.2.10, segue que

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \cdot [\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}]$$

Como $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, é suficiente mostrar que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Para isso, considere $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$. Note que ζ_n é uma raiz de $f(x)$. Ainda, $f(x)$ é irredutível sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Portanto, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$. Assim,

$$\begin{aligned} [\mathbb{Q}(\zeta_n) : \mathbb{Q}] &= [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \cdot [\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] \Rightarrow \\ \varphi(n) &= 2 \cdot [\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] \Rightarrow [\mathbb{Q}(\zeta_n + \zeta_n^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}, \end{aligned}$$

o que prova o resultado. □

Note que uma consequência direta da Proposição 5.1.17, é que

$$\left\{ 1, \zeta_n + \zeta_n^{-1}, (\zeta_n + \zeta_n^{-1})^2, \dots, (\zeta_n + \zeta_n^{-1})^{\frac{\varphi(n)}{2}-1} \right\}$$

é uma base da extensão $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Portanto,

$$\left\{ 1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-(\frac{\varphi(n)}{2}-1)} \right\}$$

também é uma base da extensão $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Definição 5.1.18. O corpo $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é chamado **subcorpo maximal real** de $\mathbb{Q}(\zeta_n)$.

5.2 Anel de inteiros de $\mathbb{Q}(\zeta_n)$

Nesta seção, iremos calcular o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ do corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_n)$. Para isso, obtemos alguns casos, sendo quando $n = p$ é um primo, quando $n = p^r$ é uma potência de um primo e, por fim, o caso que nos interessa, quando n é qualquer. Começamos com o caso em que $n = p$ primo.

Observação 5.2.1. Note que os conjugados de ζ_p são os elementos $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$. Logo,

$$\phi_p(\zeta_p) = 0 \Rightarrow \zeta_p^{p-1} + \dots + \zeta_p + 1 = 0.$$

Por definição, segue que o traço é a soma dos conjugados. Assim,

$$\begin{aligned} (\zeta_p^{p-1} + \dots + \zeta_p) + 1 &= \text{Tr}_{\mathbb{Q}(\zeta_p)}(\zeta_p^i) + 1 = 0 \Rightarrow \\ \text{Tr}_{\mathbb{Q}(\zeta_p)}(\zeta_p^i) &= -1, \text{ para todo } i = 1, 2, \dots, p-1. \end{aligned}$$

Lema 5.2.2. Se ζ_p é uma raiz p -ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde p é um número primo, então

1. $Tr_{\mathbb{K}}(\zeta_p^j) = -1$, para $j = 1, \dots, p-1$.
2. $Tr_{\mathbb{K}}(1 - \zeta_p^j) = p$, para $j = 1, \dots, p-1$.
3. $N_{\mathbb{K}}(\zeta_p - 1) = (-1)^{p-1}p$ e $N_{\mathbb{K}}(1 - \zeta_p) = p$.
4. $p = (1 - \zeta_p)(1 - \zeta_p^2) \dots (1 - \zeta_p^{p-1})$.

Demonstração. Seja ζ_p uma raiz p -ésima primitiva da unidade.

1. Pela Observação 5.2.1, segue que o p -ésimo polinômio ciclotômico de ζ_p é dado por

$$\phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1.$$

As raízes de $\phi_p(x)$ são $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$. Assim,

$$0 = \phi_p(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \dots + \zeta_p^j + 1 \Rightarrow \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \dots + \zeta_p^j = -1.$$

Portanto, $Tr_{\mathbb{K}}(\zeta_p^j) = \zeta_p^{j(p-1)} + \zeta_p^{j(p-2)} + \dots + \zeta_p^j = -1$, para $j = 1, \dots, p-1$.

2. $Tr_{\mathbb{K}}(1 - \zeta_p^j) = Tr_{\mathbb{K}}(1) - Tr_{\mathbb{K}}(\zeta_p^j)$. Como $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, segue que

$$Tr_{\mathbb{K}}(1) = 1 + 1 + \dots + 1 = p-1$$

Do item 1, segue que $Tr_{\mathbb{K}}(\zeta_p^j) = -1$. Assim, $Tr_{\mathbb{K}}(1 - \zeta_p^j) = p-1 + 1 = p$.

3. Como $\zeta_p - 1$ é uma raiz do polinômio

$$\begin{aligned} f(x) &= \phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \dots + (x+1) + 1 \\ &= x^{p-1} + \sum_{j=p-1}^1 \binom{p}{j} x^{j-1}, \end{aligned}$$

segue que $N_{\mathbb{K}}(\zeta_p - 1) = (-1)^{p-1}p$ e

$$\begin{aligned} N_{\mathbb{K}}(1 - \zeta_p) &= N_{\mathbb{K}}((-1)(\zeta_p - 1)) = N_{\mathbb{K}}(-1)N_{\mathbb{K}}(\zeta_p - 1) \\ &= (-1)^{p-1}(-1)^{p-1}p = (-1)^{2(p-1)}p = p. \end{aligned}$$

4. Como $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$ são raízes do polinômio mônico $\phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$, segue que

$$x^{p-1} + x^{p-2} + \dots + x + 1 = (x - \zeta_p)(x - \zeta_p^2) \dots (x - \zeta_p^{p-1}).$$

Assim, tomando $x = 1$, segue que

$$(1 - \zeta_p)(1 - \zeta_p^2) \dots (1 - \zeta_p^{p-1}) = p.$$

Portanto, o lema está provado. □

Lema 5.2.3. Considere $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde p é um número primo. Sejam $\mathcal{O}_{\mathbb{K}}$ anel de inteiros de $\mathbb{K}$ e $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $Tr_{\mathbb{K}}(\alpha(1 - \zeta_p)) \in p\mathbb{Z}$, para todo $\alpha \in \mathcal{O}_{\mathbb{K}}$.

Demonstração. Observe que

$$1 - \zeta_p^i = (1 - \zeta_p)(\zeta_p^{i-1} + \zeta_p^{i-2} + \cdots + \zeta_p + 1).$$

Assim, $1 - \zeta_p^i$ é um múltiplo de $1 - \zeta_p$ em $\mathcal{O}_{\mathbb{K}}$. Dessa forma, cada conjugado de $\alpha(1 - \zeta_p)$, dado por $\alpha_i(1 - \zeta_p^i)$, é um múltiplo de $(1 - \zeta_p^i)$ em $\mathcal{O}_{\mathbb{K}}$, para $i = 1, 2, \dots, p-1$. Agora, como o traço é a soma dos conjugados, segue que

$$\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p)) = \alpha_1(1 - \zeta_p) + \alpha_2(1 - \zeta_p^2) + \cdots + \alpha_p(1 - \zeta_p^p) = \beta(1 - \zeta_p),$$

onde $\beta \in \mathcal{O}_{\mathbb{K}}$. Como $\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p))$ pertence ao corpo $\mathbb{K}$ e $\mathbb{Z}$ é integralmente fechado, segue que $\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p)) \in \mathbb{Z}$. Dessa forma,

$$\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p)) \in (1 - \zeta_p)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z},$$

como queríamos. $\square$

Teorema 5.2.4. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_p)$, onde p é um número primo. O anel de inteiros de $\mathbb{K}$ é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Assim, $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$ é uma base de $\mathbb{Z}[\zeta_p]$ como um $\mathbb{Z}$ -módulo.*

Demonstração. Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{Q}(\zeta_p)$. Primeiro, mostremos que $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{K}}$. Considere $\mathbb{K} = \mathbb{Q}(\zeta_p)$. Vimos no Exemplo 5.1.9 que ζ_p é uma raiz do polinômio $x^p - 1 = (x - 1)(x^{p-1} + \cdots + x + 1)$. Como $\zeta_p \neq 1$, segue que ζ_p é uma raiz de $\phi_p(x) = (x^{p-1} + \cdots + x + 1) \in \mathbb{Z}[x]$. Em outras palavras, ζ_p é um inteiro algébrico. Como vale para qualquer p primo, segue que $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{K}}$. Agora, vamos provar que $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_p]$. Considere $\alpha \in \mathcal{O}_{\mathbb{K}} \subset \mathbb{Q}(\zeta_p)$. Assim, existem $a_0, a_1, \dots, a_{p-1} \in \mathbb{Q}$ tais que

$$\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$$

Multiplicando por $1 - \zeta_p$ em ambos os lados, segue que

$$\begin{aligned} \alpha(1 - \zeta_p) &= [a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}](1 - \zeta_p) \Rightarrow \\ \alpha(1 - \zeta_p) &= a_0(1 - \zeta_p) + a_1(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}(\zeta_p^{p-2} - \zeta_p^{p-1}). \end{aligned}$$

Pelo Lema 5.2.3, segue que $\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p)) \in p\mathbb{Z}$. Logo, existem inteiros $a_0, \dots, a_{p-2}$ tais que

$$\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p)) = a_0\text{Tr}_{\mathbb{K}}(1 - \zeta_p) + a_1\text{Tr}_{\mathbb{K}}(\zeta_p - \zeta_p^2) + \cdots + a_{p-2}\text{Tr}_{\mathbb{K}}(\zeta_p^{p-2} - \zeta_p^{p-1}) \in p\mathbb{Z}.$$

Como $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i = 1, 2, \dots, p-2$, segue que

$$a_0\text{Tr}_{\mathbb{K}}(1 - \zeta_p) = a_0p \in p\mathbb{Z},$$

onde $a_0 \in \mathbb{Z}$. Agora, $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_{\mathbb{K}}$. Assim, como $\zeta_p^{-1} = \zeta_p^{p-1} \in \mathcal{O}_{\mathbb{K}}$, segue que

$$\begin{aligned} \alpha - a_0 &= a_1\zeta_p + a_2\zeta_p^2 + a_3\zeta_p^3 + \cdots + a_{p-2}\zeta_p^{p-2} \\ \Rightarrow (\alpha - a_0)\zeta_p^{-1} &= a_1 + a_2\zeta_p + \cdots + a_{p-2}\zeta_p^{p-3}. \end{aligned}$$

Novamente, multiplicando ambos os lados da igualdade por $1 - \zeta_p$, segue que

$$(\alpha - a_0)\zeta_p^{-1}(1 - \zeta_p) = a_1(1 - \zeta_p) + a_2\zeta_p(1 - \zeta_p) + \cdots + a_{p-2}\zeta_p^{p-3}(1 - \zeta_p),$$

Aplicando o traço na igualdade acima e pelo Lema 5.2.3, segue que

$$\text{Tr}_{\mathbb{K}}((\alpha - a_0)\zeta_p^{-1}(1 - \zeta_p)) = a_1 \text{Tr}_{\mathbb{K}}(1 - \zeta_p) + a_2 \text{Tr}_{\mathbb{K}}(\zeta_p - \zeta_p^2) + \cdots + a_{p-2} \text{Tr}_{\mathbb{K}}(\zeta_p^{p-3} - \zeta_p^{p-2}) \in p\mathbb{Z}.$$

Ainda, como $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(\zeta_p^i - \zeta_p^{i+1}) = 0$, para $i = 1, 2, \dots, p-2$, segue que

$$a_1 \text{Tr}_{\mathbb{K}}(1 - \zeta_p) = a_1 p \in p\mathbb{Z},$$

onde $a_1 \in \mathbb{Z}$. Prosseguindo, desta forma, mostramos que cada a_i pertence a $\mathbb{Z}$, para cada $i = 1, \dots, n$. Assim, se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então $\alpha \in \mathbb{Z}[\zeta_p]$, isto é, $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{K}}$. $\square$

Agora, veremos o anel de inteiros de $\mathbb{Q}(\zeta_n)$ para n uma potência de primos, isto é, $n = p^r$, com p primo e r um número inteiro maior do que 1. Neste caso, o p^r -ésimo polinômio ciclotômico é dado por

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{\phi_1(x)\phi_2(x)\cdots\phi_{p^{r-1}}(x)} = \frac{x^{p^r-1}}{x^{p^{r-1}} - 1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + \cdots + x^{p^{r-1}} + 1.$$

Isso nos permite reescrever o Lema 5.2.3 da seguinte forma.

Lema 5.2.5. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_p^r)$, onde p é um número primo e r é um inteiro maior que 1. Se $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de $\mathbb{Q}$ em $\mathbb{K}$, e $\alpha \in \mathcal{O}_{\mathbb{K}}$, então*

1. $(1 - \zeta_p^r)\mathcal{O}_{\mathbb{K}} \cap \mathbb{Z} = p\mathbb{Z} = \langle p \rangle$.
2. $\text{Tr}_{\mathbb{K}}(\alpha(1 - \zeta_p^r)) \in p\mathbb{Z}$, para todo $\alpha \in \mathcal{O}_{\mathbb{K}}$.

Demonstração. A demonstração é análoga a feita no Lema 5.2.3. $\square$

Mostramos a seguir que o anel de inteiros de $\mathbb{Q}(\zeta_{p^r})$ é dado por $\mathbb{Z}[\zeta_{p^r}]$. Para isso, precisamos dos seguintes resultados.

Proposição 5.2.6. *Se $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um inteiro maior que 1, então*

1. $N_{\mathbb{K}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$,
2. $\text{Tr}_{\mathbb{K}}(\zeta_{p^r}^j) = -1$,
3. $\text{Tr}_{\mathbb{K}}(a) = (p-1)p^{r-1}a$, onde $a \in \mathbb{Q}$,
4. $N_{\mathbb{K}}(a) = a^{(p-1)p^{r-1}}$, onde $a \in \mathbb{Q}$,
5. $\prod_k (1 - \zeta_{p^r}^k) = p$, com $1 \leq k \leq p^r$, e tal que $p \nmid k$. Em particular, $N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_{p^r}) = p$,
6. $T_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_{p^r}) = (p-1)p^{r-1} + 1$.

Demonstração. Por definição, segue que

1. $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = \zeta_{p^r}^j \zeta_{p^r}^{j+1} \cdots \zeta_{p^r}^{j+(p-1)p^{r-1}}$. Como $\zeta_{p^r}^j$ e $\zeta_{p^r}^{j+p^{r-1}}$ são elementos conjugados, segue que

$$\zeta_{p^r}^j \zeta_{p^r}^{j+1} \cdots \zeta_{p^r}^{j+(p-1)p^{r-1}} = (-1)^{(p-1)p^{r-1}}.$$

Portanto, $N_{\mathbb{K}/\mathbb{Q}}(\zeta_{p^r}^j) = (-1)^{(p-1)p^{r-1}}$, para $j = 0, \dots, p^{r-1}$ e $\text{mdc}(j, p^r) = 1$. Como $\phi_{p^r}(\zeta_{p^r}^j) = \zeta_{p^r}^j + \zeta_{p^r}^{j+1} + \cdots + \zeta_{p^r}^{j+(p-1)p^{r-1}} + 1 = 0$, segue que

$$\zeta_{p^r}^j + \zeta_{p^r}^{j+1} + \cdots + \zeta_{p^r}^{j+(p-1)p^{r-1}} = -1.$$

Portanto, $\text{Tr}_{\mathbb{K}}(\zeta_{p^r}^j) = -1$.

2. $Tr_{\mathbb{K}}(a) = a + a + \cdots + a = (p-1)p^{r-1}a.$

3. $N_{\mathbb{K}}(a) = aa \dots a = a^{(p-1)p^{r-1}}.$

4. Como

$$\phi_{p^r}(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}},$$

segue que todos os $\zeta_{p^r}^k$, onde $1 \leq k \leq p^r$ e tal que $p \nmid k$, são raízes de $\phi_{p^r}(x)$ uma vez que são raízes de $x^{p^r} - 1$ mas não de $x^{p^{r-1}} - 1$. Deste modo,

$$\phi_{p^r}(x) = \prod_k (x - \zeta_{p^r}^k)$$

e existem exatamente $\varphi(p^r) = (p-1)p^{r-1}$ valores de k , uma vez que $\deg(\phi_{p^r}(x)) = (p-1)p^{r-1}$. Tomando $x = 1$, segue que

$$\phi_{p^r}(1) = \prod_{k=1, p \nmid k}^{p^r} (1 - \zeta_{p^r}^k) = 1 + 1^{p^{r-1}} + \cdots + 1^{(p-1)p^{r-1}} = p.$$

Portanto, $\prod_{k=1, p \nmid k}^{p^r} (1 - \zeta_{p^r}^k) = p$. Agora, como $N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_{p^r}) = \prod_{j=1, p \nmid j}^{p^r} (1 - \zeta_{p^r}^j)$, segue que $N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta_{p^r}) = p$.

5. Como $Tr_{\mathbb{K}}(1 - \zeta_{p^r}) = Tr_{\mathbb{K}}(1) - T_{\mathbb{K}}(\zeta_{p^r})$, pelo item 3, segue que $Tr_{\mathbb{K}}(1) = (p-1)p^{r-1}$ e pelo item 2, que $Tr_{\mathbb{K}}(\zeta_{p^r}) = -1$. Portanto, $Tr_{\mathbb{K}}(1 - \zeta_{p^r}) = (p-1)p^{r-1} + 1$,

o que prova a proposição. $\square$

Lema 5.2.7. $\mathbb{Z}[1 - \zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$.

Demonstração. Por definição, segue que $\mathbb{Z}[\alpha] = \{f(\alpha) : f(x) \in \mathbb{Z}[x]\}$. Assim, para todo $\alpha \in \mathbb{Z}[1 - \zeta_{p^r}]$, segue que

$$\begin{aligned} \alpha &= a_0 + a_1(1 - \zeta_{p^r}) + a_2(1 - \zeta_{p^r})^2 + \cdots + a_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}} \\ &= (a_0 + a_1 + \cdots + a_{(p-1)p^{r-1}}) + (-a_1 - 2a_2)\zeta_{p^r} + \cdots \end{aligned}$$

Assim, $\alpha = b_0 + b_1\zeta_{p^r} + b_2\zeta_{p^r}^2 + \cdots + b_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$, e portanto, $\alpha \in \mathbb{Z}[\zeta_{p^r}]$. Agora, se $\alpha \in \mathbb{Z}[\zeta_{p^r}]$, então $\alpha = a_0 + a_1\zeta_{p^r} + a_2\zeta_{p^r}^2 + \cdots + a_{(p-1)p^{r-1}}\zeta_{p^r}^{(p-1)p^{r-1}}$. Como $\zeta_{p^r} = 1 - (1 - \zeta_{p^r})$, segue que α pode ser escrito da forma

$$\begin{aligned} \alpha &= a_0 + a_1(1 - (1 - \zeta_{p^r})) + a_2(1 - (1 - \zeta_{p^r}))^2 + \cdots + a_{(p-1)p^{r-1}}(1 - (1 - \zeta_{p^r}))^{(p-1)p^{r-1}} \\ &= a_0 + a_1 - a_1(1 - \zeta_{p^r}) + a_2(1 - 2(1 - \zeta_{p^r}) + (1 - \zeta_{p^r})^2) + \cdots \\ &= a_0 + a_1 - a_1(1 - \zeta_{p^r}) + a_2 - 2a_2(1 - \zeta_{p^r}) + a_2(1 - \zeta_{p^r})^2 + \cdots \\ &= (a_0 + a_1 + a_2 + \cdots + a_{(p-1)p^{r-1}-1}) + (-a_1 - 2a_2 - \cdots - ((p-1)p^{r-1} - 1)a_{(p-1)p^{r-1}-1}) \\ &\quad (1 - \zeta_{p^r}) + (a_2 - 3a_3 + \cdots)(1 - \zeta_{p^r})^2 + \cdots, \end{aligned}$$

ou seja,

$$\alpha = b_0 + b_1(1 - \zeta_{p^r}) + b_2(1 - \zeta_{p^r})^2 + \cdots + b_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}} \in \mathbb{Z}[1 - \zeta_{p^r}].$$

Portanto, $\mathbb{Z}[\zeta_{p^r}] = \mathbb{Z}[1 - \zeta_{p^r}]$. $\square$

Lema 5.2.8. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um inteiro maior que 1. Se $D_{\mathbb{K}}(1, \zeta_{p^r}, \dots, \zeta_{p^r}^{(p-1)p^{r-1}-1}) = d$, então $d = p^s$ para algum $s \in \mathbb{N}$.*

Demonstração. Seja ϕ_{p^r} o p^r -ésimo polinômio ciclotômico. Assim,

$$\phi_{p^r}(x) = \frac{x^{p^r-1}}{x^{p^{r-1}}-1} \Rightarrow x^{p^r} - 1 = \phi_{p^r}(x)g(x), \quad (5.1)$$

onde $g(x) = x^{p^{r-1}} - 1$. Derivando ambos os lados da Equação obtida em (5.1), segue que

$$p^r x^{p^r-1} = \phi'_{p^r}(x)g(x) + \phi_{p^r}(x)g'(x),$$

Agora, vamos substituir x por ζ_{p^r} , segue que

$$\begin{aligned} p^r \zeta_{p^r}^{p^r-1} &= \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}) + \phi_{p^r}(\zeta_{p^r})g'(\zeta_{p^r}) \xrightarrow{\phi_{p^r}(\zeta_{p^r})=0} \\ p^r \zeta_{p^r}^{p^r-1} &= \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}), \end{aligned}$$

ou seja,

$$p^r \zeta_{p^r}^{p^r-1} = \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}).$$

Logo,

$$p^r = \zeta_{p^r} \phi'_{p^r}(\zeta_{p^r})g(\zeta_{p^r}),$$

e aplicando a função norma em ambos os lados da última igualdade, segue que

$$p^{(p-1)p^{r-1}r} = N_{\mathbb{K}}(\phi'_{p^r}(\zeta_{p^r}))N_{\mathbb{K}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Assim, pela Proposição 2.5.14, segue que

$$p^{(p-1)p^{r-1}r} = \pm D_{\mathbb{K}}(1, \zeta_{p^r}, \dots, \zeta_{p^r}^{(p-1)p^{r-1}-1})N_{\mathbb{K}}(\zeta_{p^r}g(\zeta_{p^r})).$$

Portanto, $d \mid p^{r(p-1)p^{r-1}}$, ou seja, $d = p^s$, para algum inteiro s . $\square$

Teorema 5.2.9. *Sejam $\mathbb{K}$ uma extensão finita de grau n de $\mathbb{Q}$, $\{\alpha_1, \dots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, onde $\alpha_i \in \mathcal{O}_{\mathbb{K}}$ e $D_{\mathbb{K}}(\alpha_1, \dots, \alpha_n) = d$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então α pode ser escrito na forma*

$$\alpha = \frac{m_1\alpha_1 + \dots + m_n\alpha_n}{d},$$

com $m_j \in \mathbb{Z}$ e m_j^2 divisível por d , para $j = 1, 2, \dots, n$.

Demonstração. Seja $\alpha \in \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{K}$, segue que $\alpha \in \mathbb{K}$. Sendo $\{\alpha_1, \dots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue que α pode ser escrito na forma

$$\alpha = x_1\alpha_1 + \dots + x_n\alpha_n,$$

com $x_j \in \mathbb{Q}$, para $j = 1, \dots, n$. Sejam $\sigma_1, \dots, \sigma_n$ os $\mathbb{Q}$ -monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Aplicando σ_i , para cada $i = 1, \dots, n$, em α , obtemos um sistema de n equações dado por

$$\sigma_i(\alpha) = x_1\sigma_i(\alpha_1) + \dots + x_n\sigma_i(\alpha_n),$$

para $i = 1, \dots, n$, ou seja,

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix}.$$

Resolvendo esse sistema pela regra de Cramer, segue que as n raízes são dadas por $x_j = \frac{\gamma_j}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_j é obtido de δ trocando a j -ésima coluna por $\sigma_i(\alpha)$. Assim, os γ_j , para $j = 1, 2, \dots, n$, e δ são inteiros algébricos uma vez que são obtidos a partir dos α_i 's, que são, por hipótese, inteiros algébricos. Pela Proposição 2.5.12, segue que $\delta^2 = d$, e portanto,

$$dx_j = d \frac{\gamma_j}{\delta} = \delta^2 \frac{\gamma_j}{\delta} = \delta \gamma_j$$

é um inteiro algébrico. Como $\mathbb{Z}$ é integralmente fechado, segue que $dx_j \in \mathbb{Z}$, para $j = 1, 2, \dots, n$. Seja $m_j = dx_j$, para $j = 1, 2, \dots, n$. Se mostrarmos que $\frac{m_j^2}{d} \in \mathbb{Z}$, segue que m_j^2 é divisível por d . Mas, como $\frac{m_j^2}{d} \in \mathbb{Q}$ e como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, segue que é suficiente mostrarmos que $\frac{m_j^2}{d}$ é um inteiro algébrico. Como $m_j = dx_j = \delta \gamma_j$, segue que $m_j^2 = d^2 x_j^2 = \delta^2 \gamma_j^2 = d \gamma_j^2$. Logo, $\frac{m_j^2}{d} = \gamma_j^2$ é um inteiro algébrico pois γ_j é um inteiro algébrico. Portanto

$$\frac{m_j^2}{d} \in \mathbb{Z} \Rightarrow m_j^2 \text{ é divisível por } d.$$

Assim, $\alpha = \frac{m_1 \alpha_1 + \dots + m_n \alpha_n}{d}$, com $m_j \in \mathbb{Z}$ e m_j^2 divisível por d , para $j = 1, 2, \dots, n$. $\square$

Teorema 5.2.10. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_{p^r})$, onde p é um número primo e r é um inteiro maior que 1. O anel de inteiros de $\mathbb{K}$ é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$ e $\{1, \zeta_{p^r}, \dots, \zeta_{p^r}^{(p-1)p^{r-1}-1}\}$ é uma base de $\mathbb{Z}[\zeta_{p^r}]$ como um $\mathbb{Z}$ -módulo.*

Demonstração. Vimos no Lema 5.2.7, que $\mathbb{Z}[1 - \zeta_{p^r}] = \mathbb{Z}[\zeta_{p^r}]$. Assim, basta mostrar que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[1 - \zeta_{p^r}]$ e segue o resultado. Claramente $\mathbb{Z}[1 - \zeta_{p^r}] \subseteq \mathcal{O}_{\mathbb{K}}$. Suponha que $\mathcal{O}_{\mathbb{K}} \neq \mathbb{Z}[1 - \zeta_{p^r}]$, isto é, $\mathbb{Z}[1 - \zeta_{p^r}] \subsetneq \mathcal{O}_{\mathbb{K}}$. Seja $\alpha \in \mathcal{O}_{\mathbb{K}} \setminus \mathbb{Z}[1 - \zeta_{p^r}]$. Pelo Teorema 5.2.9 e pelo Lema 5.2.8, segue que

$$\alpha = \frac{m_0 + m_1(1 - \zeta_{p^r}) + \dots + m_{(p-1)p^{r-1}-1}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s}, \quad (5.2)$$

onde $m_i \in \mathbb{Z}$, para $i = 1, 2, \dots, (p-1)p^{r-1}$. Como $\mathbb{Z}[1 - \zeta_{p^r}] \subsetneq \mathcal{O}_{\mathbb{K}}$, segue que nem todos os m_i 's são divisíveis por p^s . Tome j o menor índice tal que m_j não seja divisível por p^s . Dessa forma, fazendo a divisão dos índices que são divisíveis por p^s , resta η da seguinte forma:

$$\eta = \frac{m_0 + m_1(1 - \zeta_{p^r}) + \dots + m_{j-1}(1 - \zeta_{p^r})^{j-1}}{p^s} \in \mathbb{Z}[1 - \zeta_{p^r}] \subseteq \mathcal{O}_{\mathbb{K}} \quad (5.3)$$

Assim,

$$\beta = \alpha - \eta = \frac{m_j(1 - \zeta_{p^r})^j + \dots + m_{(p-1)p^{r-1}-1}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1}}{p^s} \in \mathcal{O}_{\mathbb{K}}. \quad (5.4)$$

Multiplicando ambos os lados por p^{s-1} , obtemos

$$\gamma = \beta p^{s-1} = \frac{m_j(1 - \zeta_{p^r})^j + m_{j+1}(1 - \zeta_{p^r})^{j+1} + \dots + m_{(p-1)p^{r-1}-1}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1}}{p}$$

Note que este é um elemento de $\mathcal{O}_{\mathbb{K}}$, onde $m_i \in \mathbb{Z}$, para $i = j, j+1, \dots, (p-1)p^{r-1}-1$, e m_j não é divisível por p . Agora, pela Proposição 5.2.6, segue que $\prod_k (1 - \zeta_{p^r}^k) = p$, onde $1 \leq k \leq p^r$ e $p \nmid k$. Seja y_t um elemento de $\mathbb{Z}[1 - \zeta_{p^r}]$. Assim, $1 - \zeta_{p^r}^t = (1 - \zeta_{p^r})y_t$, para $t = 1, 2, \dots, (p-1)p^{r-1}$. Logo,

$$\frac{p}{(1 - \zeta_{p^r})^t} = \frac{\prod_k (1 - \zeta_{p^r}^k)}{(1 - \zeta_{p^r})^t} = \frac{(1 - \zeta_{p^r})^t y_t}{(1 - \zeta_{p^r})^t} \in \mathbb{Z}[1 - \zeta_{p^r}].$$

onde $y_t \in \mathbb{Z}[1 - \zeta_{p^r}]$. Assim,

$$\begin{aligned} \gamma \frac{p}{(1 - \zeta_{p^r})^{j+1}} &= \frac{m_j}{1 - \zeta_{p^r}} + m_{j+1} + m_{j+2}(1 - \zeta_{p^r}) + \dots + m_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1-j} \Rightarrow \\ \frac{m_j}{1 - \zeta_{p^r}} &= \gamma \frac{p}{(1 - \zeta_{p^r})^j} - (m_{j+1} + m_{j+2}(1 - \zeta_{p^r}) + \dots + m_{(p-1)p^{r-1}}(1 - \zeta_{p^r})^{(p-1)p^{r-1}-1-j}), \end{aligned}$$

é um elemento de $\mathcal{O}_{\mathbb{K}}$, ou seja, $m_j = (1 - \zeta_{p^r})z$, onde $z \in \mathcal{O}_{\mathbb{K}}$. Aplicando a norma, segue que $N_{\mathbb{K}}(m_j) = N_{\mathbb{K}}(1 - \zeta_{p^r})z = N_{\mathbb{K}}(1 - \zeta_{p^r})N_{\mathbb{K}}(z)$. Como

$$N_{\mathbb{K}}(m_j) = m_j^{(p-1)p^{r-1}}, \quad N_{\mathbb{K}}(1 - \zeta_{p^r}) = p \text{ e } N_{\mathbb{K}}(z) \in \mathbb{Z},$$

segue que $p \mid m_j^{(p-1)p^{r-1}}$. Mas, isso é um absurdo, uma vez que $p \nmid m_j$. Assim, $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[1 - \zeta_{p^r}]$. E portanto, são iguais. Assim, podemos concluir que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_{p^r}]$. $\square$

Esses resultados permitem, finalmente, mostrar o caso geral, isto é, determinar o anel de inteiros para qualquer corpo ciclotômico $\mathbb{Q}(\zeta_n)$, onde ζ_n é uma raiz n -ésima primitiva da unidade. Esta generalização segue de um resultado mais geral considerando os inteiros algébricos de um corpo composto $\mathbb{KL}$, onde $\mathbb{K}$ e $\mathbb{L}$ são corpos de números. Para isso, precisamos de algumas definições e resultados.

Definição 5.2.11. Sejam $\mathbb{K}$ e $\mathbb{L}$ corpos de números. Definimos o **corpo composto** $\mathbb{KL}$ como sendo o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e $\mathbb{L}$. Este é dado por todas as somas finitas, isto é,

$$\mathbb{KL} = \{x_1 y_1 + \dots + x_r y_r, \text{ onde } x_i \in \mathbb{K}, \text{ e } y_i \in \mathbb{L}, \text{ para } i = 1, 2, \dots, r\}.$$

Definição 5.2.12. Sejam $\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}_{\mathbb{L}}$ os anéis dos inteiros algébricos dos corpos $\mathbb{K}$ e $\mathbb{L}$, respectivamente. Definimos o **produto de** $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$ por

$$\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} = \{\alpha_1 \beta_1 + \dots + \alpha_r \beta_r : \alpha_i \in \mathcal{O}_{\mathbb{K}}, \beta_i \in \mathcal{O}_{\mathbb{L}}, \text{ para } i = 1, 2, \dots, r\}.$$

Claramente $\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} \subset \mathcal{O}_{\mathbb{KL}}$, onde $\mathcal{O}_{\mathbb{KL}}$ é o anel de inteiros do corpo composto $\mathbb{KL}$. Uma questão natural é: $\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}} = \mathcal{O}_{\mathbb{KL}}$? Em geral, a igualdade não acontece, entretanto, pode-se mostrar que $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$ sob certas condições sobre os corpos ciclotômicos.

Sejam m e n os graus de $\mathbb{K}$ e $\mathbb{L}$ sobre $\mathbb{Q}$, respectivamente, e seja $d = \text{mdc}(d_1, d_2)$, onde d_1 e d_2 são os discriminantes de $\mathcal{O}_{\mathbb{K}}$ e $\mathcal{O}_{\mathbb{L}}$, respectivamente.

Teorema 5.2.13. Se $[\mathbb{KL} : \mathbb{Q}] = mn$, então $\mathcal{O}_{\mathbb{KL}}(\mathbb{Z}) \subset \frac{1}{d}\mathcal{O}_{\mathbb{K}}\mathcal{O}_{\mathbb{L}}$.

Demonstração. Sejam $\{\alpha_1, \dots, \alpha_m\}$ uma base de $\mathcal{O}_{\mathbb{K}}$ sobre $\mathbb{Z}$ e $\{\beta_1, \dots, \beta_n\}$ uma base de $\mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{Z}$. Assim, $B = \{\alpha_i \beta_j \mid i = 1, \dots, m; j = 1, \dots, n\}$ é uma base de $\mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}$ sobre $\mathbb{Z}$ e também uma base de $\mathbb{KL}$ sobre $\mathbb{Q}$. Se $\alpha \in \mathcal{O}_{\mathbb{KL}}$, então pelo Teorema 5.2.9, segue que α pode ser escrito na forma

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r} \alpha_i \beta_j, \quad (5.5)$$

onde r e todos os m_{ij} estão em $\mathbb{Z}$. Considere, sem perda de generalidade, que $\text{mdc}(r, m_{ij}) = 1$, para todo i e j . Para mostrarmos o teorema, devemos mostrar que $r \mid d$ para qualquer α , e assim, $d = rk$, para algum $k \in \mathbb{Z}$. Desse modo,

$$\alpha = \sum_{i,j} \frac{km_{ij}}{kr} \alpha_i \beta_j = \sum_{i,j} \frac{km_{ij}}{d} \alpha_i \beta_j = \frac{1}{d} \sum_{i,j} km_{ij} \alpha_i \beta_j \in \frac{1}{d} \mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}.$$

Note que pela definição de máximo divisor comum, basta mostrar que $r \mid d_1$ e $r \mid d_2$, e assim, $r \mid d$. Agora, todo monomorfismo σ de $\mathbb{K}$ em $\mathbb{C}$ se estende a um monomorfismo (que também denotamos por σ) de $\mathbb{KL}$ em $\mathbb{C}$, fixando $\mathbb{L}$. Portanto, existem m monomorfismos e para cada σ , segue que

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r} \sigma(\alpha_i) \beta_j.$$

Se $x_i = \sum_{j=1}^n \frac{m_{ij}}{r} \beta_j$, para cada $i = 1, 2, \dots, m$, então obtemos m equações da forma

$\sum_{i=1}^m \sigma(\alpha_i) x_i = \sigma(\alpha)$ para cada σ . Escrevendo na forma matricial, segue que

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_m) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(\alpha_1) & \sigma_m(\alpha_2) & \cdots & \sigma_m(\alpha_m) \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \sigma_1(\alpha) \\ \sigma_2(\alpha) \\ \vdots \\ \sigma_m(\alpha) \end{bmatrix}.$$

Observe que podemos resolver esse sistema pela regra de Cramer, de modo que $x_i = \frac{\gamma_i}{\delta}$, onde $\delta = \det(\sigma_i(\alpha_j))$ e γ_i é obtido de δ trocando a i -ésima coluna por $\sigma(\alpha)$, para $i = 1, 2, \dots, m$. Os elementos $\sigma_j(\alpha_i)$ e $\sigma_j(\alpha)$ são inteiros algébricos e $\delta^2 = d_1$. Dessa forma, tanto δ quanto todos os γ_i são também inteiros algébricos. Agora, $d_1 x_i = d_1 \frac{\gamma_i}{\delta^2} = \delta \gamma_i \in \mathcal{O}_{\mathbb{C}}$, onde $\mathcal{O}_{\mathbb{C}}$ é o anel de inteiros algébricos de $\mathbb{C}$, e portanto,

$$d_1 x_i = \sum_{j=1}^n \frac{d_1 m_{ij}}{r} \beta_j \in \mathcal{O}_{\mathbb{C}} \cap \mathbb{L} = \mathcal{O}_{\mathbb{L}}.$$

Como $\{\beta_1, \beta_2, \dots, \beta_n\}$ forma uma base integral para $\mathcal{O}_{\mathbb{L}}$, segue que os números racionais $\frac{d_1 m_{ij}}{r}$ devem ser inteiros. Assim, r divide $(d_1 \cdot m_{ij})$, para todo i e j . Como tomamos $\text{mdc}(r, m_{ij}) = 1$, segue que $r \mid d_1$. De maneira análoga, $r \mid d_2$. Portanto, $r \mid d_1$ e $r \mid d_2$, e, consequentemente, $r \mid d$. Dessa forma, $\mathcal{O}_{\mathbb{KL}} \subseteq \frac{1}{d} \mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}$. $\square$

Corolário 5.2.14. Se $[\mathbb{KL} : \mathbb{Q}] = mn$ e $d = 1$, então $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}$.

Demonstração. Como $\mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}} \subseteq \mathcal{O}_{\mathbb{KL}}$, pelo Teorema 5.2.13, segue que $\mathcal{O}_{\mathbb{KL}} \subseteq \frac{1}{d} \mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}$. Como $d = 1$, segue que $\mathcal{O}_{\mathbb{KL}} \subseteq \mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}$. Portanto, $\mathcal{O}_{\mathbb{KL}} = \mathcal{O}_{\mathbb{K}} \mathcal{O}_{\mathbb{L}}$. $\square$

Seja $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} > 2$, onde os p_i 's são primos distintos e os $e_i \geq 1$, para todo $i = 1, 2, \dots, s$.

Lema 5.2.15. $D_{\mathbb{K}}(1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1})$ divide $n^{\varphi(n)}$.

Demonstração. Considere $x^n - 1 = \phi_n(x)g(x)$. Derivando essa equação, obtemos

$$nx^{n-1} = \phi'_n(x)g(x) + \phi_n(x)g'(x),$$

e aplicando ζ_n , segue que

$$n\zeta_n^{n-1} = \phi'_n(\zeta_n)g(\zeta_n) + \phi_n(\zeta_n)g'(\zeta_n) \Rightarrow n = \zeta_n \phi'_n(\zeta_n)g(\zeta_n).$$

Lembre que $D_{\mathbb{K}}(1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}) = \pm N_{\mathbb{K}}(\phi'(\zeta_n))$. Assim, aplicando a norma, obtemos

$$n^{\varphi(n)} = N_{\mathbb{K}}(\phi'(\zeta_n))N_{\mathbb{K}}(\zeta_n g(\zeta_n)) \Rightarrow n^{\varphi(n)} = \pm D_{\mathbb{K}}(1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1})N_{\mathbb{K}}(\zeta_n g(\zeta_n)),$$

Portanto, $D_{\mathbb{K}}(1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1})$ divide $n^{\varphi(n)}$. $\square$

Teorema 5.2.16. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_n)$, onde $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} > 2$, p_i 's são primos distintos e $e_i \geq 1$, para todo $i = 1, 2, \dots, s$. O anel de inteiros de $\mathbb{K}$, é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n]$ e $\{1, \zeta_n, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ como um $\mathbb{Z}$ -módulo.*

Demonstração. Seja $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} > 2$. A prova é feita por indução sobre s . Se $s = 1$, então $n = p^e$, com p um primo. Pelo Teorema 5.2.10, segue que o anel de inteiros de $\mathbb{Q}(\zeta_{p^e})$ é $\mathbb{Z}[\zeta_{p^e}]$. Como hipótese de indução, suponha que o resultado vale para $s - 1$. Mostremos que o resultado vale para s . Sejam p um primo divisor de n e p^k a maior potência de p que divide n . Assim, $n = p^k m$, onde m não é divisível por p , ou seja, $\text{mdc}(m, p^k) = 1$. Pela relação de Bezout, segue que existem inteiros a e b tais que $ap^k + bm = 1$. Desse modo,

$$\zeta_n = \zeta_n^{ap^k} \zeta_n^{bm}, \text{ com } (\zeta_n^{ap^k})^m = 1 \text{ e } (\zeta_n^{bm})^{p^k} = 1.$$

Seja ζ_m uma raiz m -ésima primitiva da unidade e η uma raiz p^k -ésima primitiva da unidade. Assim, $\zeta_n^{ap^k}$ é uma potência de ζ_m e ζ_n^{bm} é uma potência de η . Portanto, obtemos o corpo composto $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\eta)$. Pelo Teorema 5.2.10, segue que $\mathcal{O}_{\mathbb{Q}(\eta)} = \mathbb{Z}[\eta]$, e, pela hipótese de indução, segue que $\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m]$. Agora, pelo Lema 5.2.15, segue que

$$\begin{aligned} d_1 &= D_{\mathbb{K}}(1, \eta, \dots, \eta^{\varphi(p^k)-1}) \mid (p^k)^{\varphi(p^k)}, \\ d_2 &= D_{\mathbb{K}}(1, \zeta_m, \dots, \zeta_m^{\varphi(m)-1}) \mid m^{\varphi(m)}. \end{aligned}$$

Desse modo, $\text{mdc}(d_1, d_2) = 1$. Finalmente, pelo Corolário 5.2.14, segue que

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathcal{O}_{\mathbb{Q}(\eta)}\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\eta]\mathbb{Z}[\zeta_m] = \mathbb{Z}[\eta, \zeta_m] = \mathbb{Z}[\zeta_n],$$

o que prova o teorema. $\square$

Agora, vamos abordar mais detalhes sobre o subcorpo ciclotômico maximal dado por $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Sabemos que $\mathbb{Q}(\zeta_n)$ é uma extensão galoisiana de $\mathbb{Q}$. Além disso,

$$\mathbb{Z}_n^* \simeq \text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}).$$

Portanto, $\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ é um grupo abeliano. Neste caso, $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ é uma extensão abeliana. Assim, segue que $\mathbb{Q}(\zeta_n)$ é um corpo de números abeliano.

Como vimos, se ζ_n é uma raiz n -ésima primitiva da unidade, então $\zeta_n + \zeta_n^{-1}$ é um número real, para $n > 2$. De fato, como ζ_n^{-1} é o conjugado complexo de ζ_n em $\mathbb{C}$. Logo, $\zeta_n + \zeta_n^{-1}$ é igual a duas vezes a parte real de ζ_n . Portanto, $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é um subcorpo de $\mathbb{Q}(\zeta_n)$ que está contido em $\mathbb{R}$.

Como ζ_n não é real, com $n > 2$, segue que o polinômio $p(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1$ é irreduzível sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ e tem ζ_n como raiz. Logo, $p(x)$ é o polinômio minimal de ζ_n sobre $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Portanto, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$.

Proposição 5.2.17. *O anel de inteiros de $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$.*

Demonstração. Sabemos que o anel de inteiros de $\mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$ pelo Teorema 5.2.16. Como ζ_n é inteiro, segue que ζ_n^{-1} é inteiro e pela Proposição 2.1.15, segue que $\zeta_n + \zeta_n^{-1}$ também é inteiro. Portanto, $\mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subseteq \mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Agora, mostremos que $\mathcal{O}_{\mathbb{K}} \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. Se $\alpha \in \mathcal{O}_{\mathbb{K}}$, então

$$\begin{aligned} \alpha &= a_0 + a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{\frac{\varphi(n)}{2}-1} \left(\zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1} \right) \\ &= a_0 + a_1\zeta_n + a_1\zeta_n^{-1} + a_2\zeta_n^2 + a_2\zeta_n^{-2} + \cdots + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{\frac{\varphi(n)}{2}-1} + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{-\frac{\varphi(n)}{2}+1}, \end{aligned}$$

onde $a_i \in \mathbb{Q}$, para $i = 0, 1, 2, \dots, \frac{\varphi(n)}{2} - 1$. Devemos mostrar que $a_i \in \mathbb{Z}$. Multiplicando α por $\zeta_n^{\frac{\varphi(n)}{2}-1}$, segue que

$$\zeta_n^{\frac{\varphi(n)}{2}-1}\alpha = a_0\zeta_n^{\frac{\varphi(n)}{2}-1} + a_1\zeta_n^{\frac{\varphi(n)}{2}} + a_1\zeta_n^{\frac{\varphi(n)}{2}-2} + a_2\zeta_n^{\frac{\varphi(n)}{2}+1} + a_2\zeta_n^{\frac{\varphi(n)}{2}-3} + \cdots + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{\varphi(n)-2} + a_{\frac{\varphi(n)}{2}-1},$$

que é um inteiro algébrico em $\mathbb{Q}(\zeta_n)$, e assim, pertence a $\mathbb{Z}[\zeta_n]$. Assim, $a_i \in \mathbb{Z}$, para $i = 0, 1, 2, \dots, \frac{\varphi(n)}{2} - 1$. Portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$, ou seja, o anel de inteiros de $\mathbb{K}$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. $\square$

Corolário 5.2.18. *$\left\{1, \zeta_n + \zeta_n^{-1}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1}\right\}$ é uma base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ como um $\mathbb{Z}$ -módulo.*

Demonstração. Como $\left\{1, \zeta_n + \zeta_n^{-1}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1}\right\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ e como

$$\left\{1, \zeta_n + \zeta_n^{-1}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1}\right\} \subseteq \mathbb{Z}[\zeta_n + \zeta_n^{-1}] \subseteq \mathcal{O}_{\mathbb{K}},$$

segue que é suficiente mostrar que é linearmente independente. Para isso, sejam os elementos $a_0, a_1, a_2, \dots, a_{\frac{\varphi(n)}{2}-1} \in \mathbb{Z}$ e suponhamos que

$$a_0 + a_1(\zeta_n + \zeta_n^{-1}) + a_2(\zeta_n^2 + \zeta_n^{-2}) + \cdots + a_{\frac{\varphi(n)}{2}-1} \left(\zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1} \right) = 0.$$

Logo,

$$\begin{aligned} 0 &= a_0 + a_1\zeta_n + a_1\zeta_n^{-1} + a_2\zeta_n^2 + a_2\zeta_n^{-2} + \cdots + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{\frac{\varphi(n)}{2}-1} + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{-\frac{\varphi(n)}{2}+1} \\ &= a_0 + a_1\zeta_n + a_1\zeta_n^{-1} + a_2\zeta_n^2 + a_2\zeta_n^{-2} + \cdots + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{\frac{\varphi(n)}{2}-1} + a_{\frac{\varphi(n)}{2}-1}\zeta_n^{n-\frac{\varphi(n)}{2}+1}. \end{aligned}$$

Como $\{1, \zeta_n, \dots, \zeta_n^{\varphi(n)-1}\}$ é uma base de $\mathbb{Z}[\zeta_n]$ sobre $\mathbb{Z}$, segue que estes elementos são linearmente independentes, e assim, $a_0 = a_1 = a_2 = \cdots = a_{\frac{\varphi(n)}{2}-1} = 0$. Desse modo,

$\left\{1, \zeta_n + \zeta_n^{-1}, \dots, \zeta_n^{\frac{\varphi(n)}{2}-1} + \zeta_n^{-\frac{\varphi(n)}{2}+1}\right\}$ é linearmente independente, e portanto, é uma base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ sobre $\mathbb{Z}$. $\square$

5.3 Unidades em corpos ciclotômicos

Já vimos que, em geral, não é uma tarefa simples explicitar o grupo das unidades de um corpo de números $\mathbb{K}$. Nesta seção, apresentamos alguns resultados sobre as unidades de corpos ciclotômicos $\mathbb{Q}(\zeta_n)$. Os Corpos Ciclotômicos são exemplos muito importantes de corpos de números e serão de grande importância no capítulo final por sua relevância no estudo da Teoria da Informação.

Primeiramente, consideramos o mais simples tipo de unidade.

Proposição 5.3.1. *Uma raiz da unidade em $\mathbb{K} = \mathbb{Q}(\zeta_n)$ é uma unidade de $\mathcal{O}_{\mathbb{K}}$.*

Demonstração. Lembre que qualquer raiz da unidade é um inteiro algébrico, uma vez que, por definição, é uma raiz do polinômio $x^m - 1$, onde $m \geq 1$. Assim, se $\zeta^m = 1$, então $\zeta^{-m} = 1$. Portanto, ζ^{-1} também é uma raiz da unidade. Dessa forma, qualquer raiz da unidade em $\mathbb{K}$ também é uma unidade de $\mathcal{O}_{\mathbb{K}}$. $\square$

Agora, considere $U_{\mathbb{K}}$ o grupo das unidades de $\mathcal{O}_{\mathbb{K}}$ e $W_{\mathbb{K}}$ o subgrupo de $U_{\mathbb{K}}$ que contém suas raízes da unidade. Observe que $W_{\mathbb{K}}$ não é um subgrupo trivial, uma vez que 1 e -1 estão contidos nele. Como não há risco de confusão neste contexto, em alguns momentos vamos adotar a notação de $U_{\mathbb{K}}$ por U e $W_{\mathbb{K}}$ por apenas W .

Sejam $\mathbb{K} = \mathbb{Q}(\zeta)$, p um primo ímpar e ζ uma raiz p -ésima primitiva da unidade. Pelo que já vimos, $\mathbb{K}$ tem grau $p - 1$ sobre $\mathbb{Q}$.

Lema 5.3.2. *Se r e s são inteiros com $\text{mdc}(p, rs) = 1$, com $1 \leq r, s \leq p - 1$, então $\frac{\zeta_p^r - 1}{\zeta_p^s - 1}$ é uma unidade de $\mathbb{Z}[\zeta_p]$.*

Demonstração. Como $\text{mdc}(p, rs) = 1$, segue que existe $t \in \mathbb{Z}$ tal que $r \equiv st \pmod{p}$, ou seja, $p \mid r - st$. Assim,

$$\frac{\zeta_p^r - 1}{\zeta_p^s - 1} = \frac{\zeta_p^{st} - 1}{\zeta_p^s - 1} = \frac{(\zeta_p^s)^t - 1}{\zeta_p^s - 1} = 1 + \zeta_p^s + \dots + \zeta_p^{s(t-1)} \in \mathbb{Z}[\zeta_p].$$

De modo análogo,

$$\frac{\zeta_p^s - 1}{\zeta_p^r - 1} \in \mathbb{Z}[\zeta_p].$$

Assim,

$$\underbrace{\frac{\zeta_p^s - 1}{\zeta_p^r - 1}}_{\in \mathbb{Z}[\zeta_p]} \cdot \underbrace{\frac{\zeta_p^r - 1}{\zeta_p^s - 1}}_{\in \mathbb{Z}[\zeta_p]} = 1,$$

o que prova o resultado. $\square$

Definição 5.3.3. As unidades dadas por $\frac{\zeta_p^r - 1}{\zeta_p^s - 1}$, onde ζ é uma raiz da unidade, são chamadas **unidades ciclotômicas**.

Lema 5.3.4. *Se p é um primo ímpar, então $p = u(1 - \zeta_p)^{p-1}$, onde u é uma unidade de $\mathbb{Z}[\zeta_p]$.*

Demonstração. Por definição, segue que

$$\phi(1) = 1^{p-1} + 1^{p-2} + \cdots + 1^1 + 1 = \prod_{i=1}^{p-1} (1 - \zeta_p^i) = p.$$

Dessa forma, o primo p pode ser escrito como $p = (1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1})$. Pelo Lema 5.3.2, vimos que $\left\{ \frac{1 - \zeta_p^i}{1 - \zeta_p^j}, \frac{1 - \zeta_p^j}{1 - \zeta_p^i} \right\}$ são unidades de $\mathbb{Z}[\zeta_p]$. Assim, se $u_i = \frac{1 - \zeta_p^i}{1 - \zeta_p} \in \mathbb{Z}[\zeta_p]$, então $1 - \zeta_p^i = u_i(1 - \zeta_p)$, onde u_i é uma unidade de $\mathbb{Z}[\zeta_p]$, para $i = 1, 2, \dots, p-1$. Portanto,

$$\begin{aligned} p &= (1 - \zeta_p)(1 - \zeta_p^2) \cdots (1 - \zeta_p^{p-1}) \\ &= u_1(1 - \zeta_p)u_2(1 - \zeta_p) \cdots u_{p-1}(1 - \zeta_p) \\ &= u(1 - \zeta_p)^{p-1}, \end{aligned}$$

onde $u = u_1 u_2 \cdots u_{p-1}$ é uma unidade de $\mathbb{Z}[\zeta_p]$. $\square$

Sejam p um primo ímpar, ζ_p uma raiz p -ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_p)$. Assim, $[\mathbb{K} : \mathbb{Q}] = p-1$ e o anel de inteiros de $\mathbb{K}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\zeta_p]$. Agora, provamos um dos resultados principais sobre unidades de $\mathbb{Q}(\zeta)$.

Teorema 5.3.5. *O grupo multiplicativo W das raízes da unidade de $\mathbb{Q}(\zeta_p)$ é dado por*

$$W = \{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}, -1, -\zeta_p, -\zeta_p^2, \dots, -\zeta_p^{p-1}\}.$$

Assim, $o(W) = \omega = 2p$ e toda unidade de $u \in \mathbb{Q}(\zeta_p)$ pode ser escrita na forma $u = \pm \zeta_p^k v$, onde v é uma unidade real positiva de $\mathcal{O}_{\mathbb{K}}$.

Demonstração. Pelo Teorema 5.1.5, vimos que o grupo W é um grupo multiplicativo cíclico de ordem finita. Considere ω a ordem de W . Como $-\zeta_p \in W$ e $-\zeta_p$ tem ordem $2p$, segue que $2p$ divide ω . Considere $x \in W$ um elemento de ordem ω , isto é, $o(x) = \omega$. Como $W \subseteq \mathbb{K}$, segue que $x \in \mathbb{K}$, e assim, $\mathbb{Q}(x) \subseteq \mathbb{K}$, deste modo,

$$\varphi(\omega) = \varphi(o(x)) = [\mathbb{Q}(x) : \mathbb{Q}] \text{ divide } p-1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}].$$

Agora, $\omega = p^r m$, onde $r \geq 1$ e $m \geq 2$, uma vez que $\omega = 2pk$, já que $2p \mid \omega$ e $p \nmid m$. Assim, como $\text{mdc}(p^r, m) = 1$, segue que

$$\varphi(\omega) = \varphi(p^r) \varphi(m) = p^{r-1}(p-1) \varphi(m),$$

uma vez que p é primo. Como $\varphi(\omega)$ divide $p-1$, segue que $p-1 = k\varphi(\omega)$, para algum $k \in \mathbb{Z}$, logo:

$$\varphi(\omega) = p^{r-1}(p-1) \varphi(m) = p^{r-1} k \varphi(\omega) \varphi(m),$$

e deste modo, $k\varphi(m)p^{r-1} = 1$, como ambos são inteiros positivos, segue que $p^{r-1} = 1$, e assim, $r = 1$ e $\varphi(m) = 1$. Como $m \geq 2$, segue que $m = 2$, ou seja, $o(W) = \omega = 2p$. Como $-1, -\zeta_p, -\zeta_p^2, \dots, -\zeta_p^{p-1}, 1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$, são raízes da unidade distintas, segue que

$$W = \{-1, -\zeta_p, -\zeta_p^2, \dots, -\zeta_p^{p-1}, 1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}.$$

Agora, seja u uma unidade de $\mathbb{K} = \mathbb{Q}(\zeta_p)$, como $\{1, \zeta_p, \zeta_p^2, \dots, \zeta_p^{p-2}\}$ é uma $\mathbb{Z}$ -base de $\mathbb{Z}[\zeta_p]$, segue que podemos escrever $u = a_0 + a_1 \zeta_p + a_2 \zeta_p^2 + \cdots + a_{p-2} \zeta_p^{p-2}$, onde $a_i \in \mathbb{Z}$ para $i = 1, 2, \dots, p-2$. O conjugado complexo de u é também uma unidade e é dado por

$$\bar{u} = a_0 + a_1 \zeta_p^{-1} + a_2 \zeta_p^{-2} + \cdots + a_{p-2} \zeta_p^{-(p-2)}.$$

Logo, $u' = u\bar{u}$ é também uma unidade, e além disso, se $u^{(k)} = a_0 + a_1\zeta_p^k + a_2\zeta_p^{2k} + \cdots + a_{p-2}\zeta_p^{k(p-2)}$, onde $k = 1, 2, \dots, p-1$, são os conjugados de u , então os conjugados de $\bar{u}$ são

$$\begin{aligned}\bar{u}^{(k)} = \sigma_k(\bar{u}) &= a_0 + a_1\zeta_p^{-k} + \cdots + a_{p-2}\zeta_p^{-k(p-2)} \\ &= a_0 + a_1(\overline{\zeta_p^k}) + \cdots + a_{p-2}(\overline{\zeta_p^{k(p-2)}}) \\ &= \overline{u^k}.\end{aligned}$$

Assim, os conjugados de u' são dados por $(u')^{(k)} = \sigma_k(u') = \sigma_k(u\bar{u}^{-1}) = \sigma_k(u)\sigma_k(\bar{u}^{-1}) = u^{(k)}[\bar{u}^{(k)}]^{-1} = u^{(k)}\overline{u^{(k)}}^{-1}$. Logo,

$$|(u')^{(k)}| = |u^{(k)}\overline{u^{(k)}}^{-1}| = |u^{(k)}u^{(k)-1}| = |u^{(k)}u^{(k)-1}| = |1| = 1,$$

com $k = 1, 2, \dots, p-1$. Pelo Corolário 5.1.4, segue que u' é uma raiz da unidade, e portanto, devemos ter $u' = \pm\zeta_p^h$, com $0 \leq h \leq p-1$, afirmamos que $u' = \zeta_p^h$. De fato, suponhamos que $u' = -\zeta_p^h$ e consideramos o homomorfismo canônico

$$\begin{aligned}\theta : \mathbb{Z}[\zeta_p] &\longrightarrow \frac{\mathbb{Z}[\zeta_p]}{(1-\zeta_p)\mathbb{Z}[\zeta_p]} \\ x &\longmapsto \theta(x) = x + (1-\zeta_p)\mathbb{Z}[\zeta_p] = [x],\end{aligned}$$

onde $[x]$ representa a classe de equivalência de x em $\frac{\mathbb{Z}[\zeta_p]}{(1-\zeta_p)\mathbb{Z}[\zeta_p]}$. Agora, como $1-\zeta_p \in (1-\zeta_p)\mathbb{Z}[\zeta_p]$, segue que $[1-\zeta_p] = 0$ em $\frac{\mathbb{Z}[\zeta_p]}{(1-\zeta_p)\mathbb{Z}[\zeta_p]}$, assim, $\theta(\zeta_p) = [\zeta_p] = [1] = 1$, e deste modo, $\theta(\zeta_p^k) = \theta(\zeta_p)^k = 1$, para $k = 1, 2, \dots, p-2$. Além disso,

$$\begin{aligned}\theta(u) &= \theta(a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-2}\zeta_p^{p-2}) \\ &= a_0 + a_1\theta(\zeta_p) + a_2\theta(\zeta_p)^2 + \cdots + a_{p-2}\theta(\zeta_p)^{p-2} \\ &= a_0 + a_1 + a_2 + \cdots + a_{p-2} = \theta(\bar{u}).\end{aligned}$$

Como $u = -\zeta_p^h\bar{u}$, segue que $\theta(u) = \theta(-\zeta_p^h\bar{u}) = -\theta(\bar{u})$, assim, tem-se que $\theta(\bar{u}) = -\theta(\bar{u})$, ou seja, $\theta(2\bar{u}) = 0$, e portanto, $2\bar{u} \in (1-\zeta_p)\mathbb{Z}[\zeta_p]$. Deste modo, existe $w \in \mathbb{Z}[\zeta_p]$ tal que $2\bar{u} = (1-\zeta_p)w$, e assim, $2 = (1-\zeta_p)wu^{-1}$. Logo, $1-\zeta_p$ divide 2 em $\mathbb{Z}[\zeta_p]$, o que implica que $(1-\zeta_p)^{p-1}$ divide 2^{p-1} . Pelo Lema 5.3.4, segue que $p = w'(1-\zeta_p)^{p-1}$, onde w' é uma unidade, e assim, $(w')^{-1}p = (1-\zeta_p)^{p-1}$, e deste modo, $p \mid (1-\zeta_p)^{p-1}$ em $\mathbb{Z}[\zeta_p]$. Logo,

$$(1-\zeta_p)^{p-1} \mid 2^{p-1} \quad \text{e} \quad p \mid (1-\zeta_p)^{p-1},$$

e assim, $p \mid 2^{p-1}$, ou seja, $p \mid 2$, o que é um absurdo, uma vez que supomos p primo ímpar. Portanto, $u' = \zeta_p^h$, e assim, $u = \zeta_p^h\bar{u}$. Agora, seja k tal que $2k \equiv h \pmod{p}$. Assim, $\zeta_p^h = \zeta_p^{2k}$, e portanto,

$$\frac{u}{\zeta_p^k} = \frac{\zeta_p^h\bar{u}}{\zeta_p^k} = \frac{\zeta_p^k\zeta_p^k\bar{u}}{\zeta_p^k} = \zeta_p^k\bar{u} = \frac{\bar{u}}{\zeta_p^{-k}} = \overline{\left(\frac{u}{\zeta_p^k}\right)} \in \mathbb{R}.$$

Seja $v = \frac{u}{\zeta_p^k} = u\zeta_p^{-k} = u\zeta_p^{p-k} \in \mathbb{Z}[\zeta_p]$. Como u e ζ_p^k são unidades segue que v é uma unidade real, e além disso,

$$u = \zeta_p^k \left(\frac{u}{\zeta_p^k} \right) = \zeta_p^k v.$$

Agora, se $v > 0$, então $u = \zeta_p^k v$, e se $v < 0$, então $v' = -v > 0$, ou seja, $u = -\zeta_p^k(-v) = -\zeta_p^k v'$, com $v' > 0$. Portanto, $u = \pm\zeta_p^k v$, onde v é uma unidade real positiva. $\square$

Agora, podemos dar um exemplo de unidades reais notáveis em $\mathbb{Q}(\zeta)$.

Exemplo 5.3.6. O elemento $\frac{1 - \zeta^s}{1 - \zeta}$ é uma unidade de $\mathbb{Q}(\zeta)$, $1 \leq s \leq p - 1$, uma vez que $1 - \zeta^s$ e $1 - \zeta$ são elementos associados. Logo, $\frac{1 - \zeta^s}{1 - \zeta} \in \mathbb{Z}[\zeta]$, que é o anel de inteiros de $\mathbb{Q}(\zeta)$.

Podemos estender o Exemplo 5.3.6 pela demonstração do Teorema 5.3.5.

Exemplo 5.3.7. Na demonstração do Teorema 5.3.5, mostramos que existe um inteiro $n = 2k$ tal que

$$\begin{aligned} \frac{1 - \zeta^s}{1 - \zeta} &= \zeta^{2k} \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}} \\ \Rightarrow \frac{1 - \zeta^s}{1 - \zeta} \cdot \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}} &= \left(\zeta^k \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}} \right)^2 \\ \Rightarrow v_s &= \sqrt{\frac{1 - \zeta^s}{1 - \zeta} \cdot \frac{1 - \zeta^{-s}}{1 - \zeta^{-1}}} \end{aligned}$$

Assim, v_s é uma unidade real em $\mathbb{Q}(\zeta)$ para todo $s = 1, 2, \dots, p - 1$.

Outro exemplo relevante são das unidades circulares, que apesar de apresentarmos, não iremos aprofundar em suas propriedades.

Exemplo 5.3.8. Considere $s \geq 1$ e $s' \leq p - 1$ tais que $s + s' = p$. Assim, $v_s = -v_{s'}$. Se $s = 1$, então $v_1 = 1$. Portanto, $v_2, v_3, \dots, v_g$, com $g = \frac{(p-1)}{2}$, são $\frac{(p-3)}{2}$ unidades reais diferentes de 1 e -1 . Logo, estas não são raízes da unidade, e assim, essas unidades são chamadas de unidades circulares.

Observação 5.3.9. Lembre que em um corpo ciclotômico, a conjugação complexa é um $\mathbb{Q}$ -automorfismo levando ζ em ζ^{-1} . O corpo fixo é $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos(2\pi/p))$, chamado de subcorpo maximal real de $\mathbb{Q}(\zeta)$.

O Teorema 5.3.10, que será apresentado a seguir afirma que qualquer unidade de $\mathbb{Z}[\zeta]$ pode ser escrita como uma raiz da unidade vezes uma unidade real, fornecendo uma relação entre as unidades de $\mathbb{Q}(\zeta)$ e as unidades do seu subcorpo maximal real $\mathbb{Q}(\zeta + \zeta^{-1})$. Esse resultado é possível já que o corpo $\mathbb{Q}(\zeta + \zeta^{-1})$ tem $\frac{p-1}{2}$ imersões reais e nenhuma complexa em $\mathbb{C}$, enquanto $\mathbb{Q}(\zeta)$ não tem imersões reais em $\mathbb{C}$ mas tem $\frac{p-1}{2}$ pares de imersões complexas. Portanto, o $\mathbb{Z}$ -posto do grupo das unidades de cada corpo é $\frac{p-3}{2}$, então as unidades de $\mathbb{Q}(\zeta + \zeta^{-1})$ são de índice finito naquelas de $\mathbb{Q}(\zeta)$. Esse Teorema pode ser justificado pelo *Teorema das Unidades de Dirichlet*. Entretanto, usamos outras estratégias para fazer a demonstração, utilizando outros resultados auxiliares.

Teorema 5.3.10. Se ϵ é uma unidade de $\mathbb{Z}[\zeta_p]$, então $\epsilon_1 \in \mathbb{Q}(\zeta + \zeta^{-1})$ e $r \in \mathbb{Z}$ tal que $\epsilon = \zeta^r \cdot \epsilon_1$.

Demonstração. Seja $\alpha = \frac{\epsilon}{\bar{\epsilon}}$. Como $\bar{\epsilon}$ também é uma unidade em $\mathbb{Z}[\zeta_p]$, segue que α é um inteiro algébrico. Agora, $\mathbb{Q}(\zeta + \zeta^{-1})$ é o Grupo de Galois de $\mathbb{Q}(\zeta)$, uma vez que é seu corpo fixo. Sabemos que toda conjugação complexa comuta com outros elementos do Grupo de

Galois, então a partir disso, segue que todos os conjugados de α tem valor absoluto 1. Pelo Corolário 5.1.4, segue que $\alpha = \frac{\epsilon}{\bar{\epsilon}}$ é uma raiz da unidade. Logo, $\frac{\epsilon}{\bar{\epsilon}} = \pm \zeta^a$, para algum a . Suponha que $\frac{\epsilon}{\bar{\epsilon}} = -\zeta^a$. Considere

$$\epsilon = b_0 + b_1\epsilon + \dots + b_{p-2}\zeta^{p-2}.$$

Assim,

$$\epsilon \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{1 - \zeta}.$$

Além disso,

$$\begin{aligned} \bar{\epsilon} &\equiv b_0 + b_i\zeta^{-1} + \dots \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{1 - \zeta} \\ \Rightarrow \bar{\epsilon} &\equiv \underbrace{\epsilon}_{-\zeta^a\bar{\epsilon}} \equiv -\bar{\epsilon} \pmod{1 - \zeta} \Rightarrow 2\bar{\epsilon} \equiv 0 \pmod{1 - \zeta}. \end{aligned}$$

Mas, note que $2 \notin \langle 1 - \zeta \rangle$. Além disso, $\langle 1 - \zeta \rangle$ é um ideal primo, e assim, $\bar{\epsilon} \in \langle 1 - \zeta \rangle$, mas isso é um absurdo, pois $\bar{\epsilon}$ é uma unidade. Logo, $\frac{\epsilon}{\bar{\epsilon}} = +\zeta^a$. Considere $2r \equiv a \pmod{p}$ e $\epsilon_1 = \zeta^{-r}\epsilon$. Assim, $\epsilon = \zeta^r\epsilon_1$ e $\epsilon_1 = \bar{\epsilon}_1$, o que prova a proposição. $\square$

A seguir, vamos adotar a seguinte notação $\mathbb{K} = \mathbb{Q}(\zeta)$, $\mathbb{K}^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. Considere $\mathcal{O}_{\mathbb{K}}^*$ o grupo das unidades do anel de inteiros de $\mathbb{K}$. Analogamente, $\mathcal{O}_{\mathbb{K}^+}^*$ é o grupo das unidades do subcorpo maximal real de $\mathbb{K}$.

No próximo teorema vamos generalizar a Proposição 5.3.10, mostrando que o índice $[\mathcal{O}_{\mathbb{K}}^* : W\mathcal{O}_{\mathbb{K}^+}^*]$ é igual a 1, quando n é uma potência de primos, ou igual a 2, se n é divisível por pelos menos dois primos distintos.

Teorema 5.3.11. *Seja $Q = [\mathcal{O}_{\mathbb{K}}^* : W\mathcal{O}_{\mathbb{K}^+}^*]$. Se n é uma potência de primo, então $Q = 1$. Caso contrário, se n não é uma potência de primos, então $Q = 2$.*

Demonstração. A demonstração para n primo ímpar é exatamente igual a dada na Proposição 5.3.10. Para $p = 2$, devemos argumentar de maneira diferente. Para isso, suponha que ϵ é uma unidade de $\mathbb{Q}(\zeta_{2^m})$ tal que $\frac{\epsilon}{\bar{\epsilon}} \notin W$. Assim, $\frac{\epsilon}{\bar{\epsilon}} = \zeta$ é uma raiz 2-ésima primitiva da unidade. Se N é a norma de $\mathbb{Q}(\zeta_{2^m})$ em $\mathbb{Q}(i)$, então

$$N(\zeta) = \zeta^a, \text{ onde } a \text{ é dado por}$$

$$a = \sum_{\substack{0 < b < 2^m \\ b \equiv 1 \pmod{4}}} = \sum_{j=0}^{2^{(m-2)}-1} (1 + 4j) = 2^{m-2} + 2^{m-1}(2^{m-2} - 1) \equiv 2^{m-2} \pmod{2^{m-1}}.$$

Portanto, ζ^a é uma 4-ésima raiz primitiva de 1 e, assim, $\zeta^a = \pm i$. Logo, $\frac{N(\epsilon)}{N(\bar{\epsilon})} = \pm 1$. Mas, $N(\epsilon)$ é uma unidade de $\mathbb{Q}(i)$, e portanto, é igual a ± 1 ou $\pm i$. Entretanto, nenhuma dessas possibilidades é satisfeita, o que é uma contradição. Logo, $Q = 1$ para $\mathbb{Q}(\zeta^{2^m})$. Agora, suponha que n não é uma potência de primos. Assim, $1 - \zeta$ é uma unidade. Contudo,

$$\frac{1 - \zeta_n}{1 - \bar{\zeta}_n} = -\zeta_n.$$

Se $-\zeta_n \in W^2$, então $-\zeta_n = (\pm \zeta_n^r)^2 = \zeta_n^{2r} \Rightarrow -1 = \zeta_n^{2r-1}$. Logo, n deve ser par, e assim, $n \equiv 0 \pmod{4}$. Como $-1 = \zeta_n^{\frac{n}{2}}$, segue que

$$\frac{n}{2} \equiv 2r - 1 \pmod{n} \Rightarrow \frac{n}{2} \equiv -1 \pmod{2},$$

o que é um absurdo, pois $n \equiv 0 \pmod{4}$. Logo, $-\zeta_n \notin W^2$. Portanto, $Q = 2$. $\square$

Podemos concluir do Teorema 5.3.11 que conhecer as unidades reais de um corpo ciclotômico é quase suficiente para conhecer todas as outras.

5.4 Unidades ciclotômicas

Apresentamos nesta seção resultados que determinam explicitamente o grupo das unidades de corpos ciclotômicos, através das chamadas unidades ciclotômicas, que tem índice finito no grupo de todas as unidades.

Na Definição 5.3.3, apresentamos as unidades ciclotômicas. A seguir, vamos definir o subgrupo das unidades ciclotômicas de $\mathbb{K} = \mathbb{Q}(\zeta_n)$.

Definição 5.4.1. Considere $n \not\equiv 2 \pmod{4}$ e sejam U_n o grupo das unidades de $\mathbb{Q}(\zeta_n)$ e V_n o grupo multiplicativo de $\mathbb{K}^+$ gerado por

$$\{\pm \zeta_n, 1 - \zeta_n^a \mid 1 \leq a \leq n - 1\}.$$

O grupo

$$C_n = V_n \cap U_n$$

é chamado **subgrupo das unidades ciclotômicas de $\mathbb{K} = \mathbb{Q}(\zeta_n)$** .

Observação 5.4.2. Se $\mathbb{K}$ é um corpo de números abeliano, então podemos definir as unidades ciclotômicas de $\mathbb{K}$ deixando $\mathbb{K} \subseteq \mathbb{Q}(\zeta_n)$, com n sendo mínimo (ou seja, o condutor de $\mathbb{K}$) e definindo $C_{\mathbb{K}} = \mathcal{O}_{\mathbb{K}} \cap C_n$. Isso funciona bem para o subcorpo maximal de $\mathbb{K}^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Como as unidades reais multiplicadas por raízes da unidade são de índice 1 ou 2 no grupo das unidades, é suficiente trabalharmos apenas com as unidades reais.

Observação 5.4.3. Se $\zeta_n = e^{\frac{2\pi i}{n}}$, então $\zeta_n^{\frac{(1-a)}{2}} \frac{1-\zeta_n^a}{1-\zeta_n} = \pm \frac{\sin(\pi a/n)}{\sin(\pi/n)}$, ou seja, é um valor real. Além disso, se mudarmos a para $-a$, então obtemos a mesma unidade multiplicada por -1 .

Proposição 5.4.4. Seja p um primo e $m \geq 1$.

1. As unidades ciclotômicas de $\mathbb{Q}(\zeta_{p^m})^+$ são geradas por -1 e pelas unidades

$$\xi_a = \zeta_{p^m}^{\frac{(1-a)}{2}} = \frac{1 - \zeta_{p^m}^a}{1 - \zeta_{p^m}}, \text{ com } 1 < a < \frac{1}{2}p^m, \text{ mdc}(a, p) = 1;$$

2. As unidades ciclotômicas de $\mathbb{Q}(\zeta_{p^m})$ são geradas por ζ_{p^m} e as unidades de $\mathbb{K}^+ = \mathbb{Q}(\zeta_{p^m})^+$.

Demonstração. Para simplificar a notação, considere ζ como ζ_{p^m} . Nesta demonstração, provamos primeiro o item 2 e depois o item 1. A definição das unidades ciclotômicas envolve $1 - \zeta^a$ para todo $a \not\equiv 0 \pmod{p^m}$. Suponha que existem $k, b \in \mathbb{Z}$ tais que $k < m$ e $\text{mdc}(b, p) = 1$. Assim, usando a seguinte relação

$$1 - x^{p^k} = \prod (1 - \zeta^{p^{m-k}} x),$$

segue que

$$1 - (\zeta^b)^{p^k} = \prod_{j=0}^{p^k-1} (1 - \zeta^{b+jp^{m-k}}).$$

Como $\text{mdc}(p, b + jp^{m-k}) = 1$, segue que podemos considerar apenas os $a \in \mathbb{Z}$ tal que $\text{mdc}(a, p) = 1$. Além disso, $1 - \zeta^a$ e $1 - \zeta^{-a}$ diferem apenas pelo fator $-\zeta^a$, isto é, uma potência de ζ , e assim, vamos apenas considerar $1 \leq a \leq \frac{1}{2}p^m$. Agora, suponha que

$$\xi = \pm \zeta^d \cdot \prod_{\substack{1 \leq a \leq \frac{1}{2}p^m \\ (a,p)=1}} (1 - \zeta^a)^{c_a} \quad (5.6)$$

é uma unidade de $\mathbb{Q}(\zeta)$. Como $(1 - \zeta_i)$ e $(1 - \zeta_j)$ são associados para todo $i, j \in \mathbb{Z}$, segue que os ideais $\langle 1 - \zeta^a \rangle$ são todos iguais. Assim, $\sum c_a = 0$, onde c_a é a potência que aparece na igualdade 5.6. Portanto,

$$\xi = \pm \zeta^d \prod \left(\frac{1 - \zeta^a}{1 - \zeta} \right)^{c_a} = \pm \zeta^e \prod_{a \neq 1} \xi_a^{c_a},$$

onde $e = d + \frac{1}{2} \sum c_a(a-1)$. Note que se $p = 2$, então para termos $\text{mdc}(a, p) = 1$, devemos ter a ímpar. Logo, $\zeta^e \in \mathbb{Q}(\zeta)$ em todos os casos. Isso completa a prova do item 2. Agora, seja $\zeta \in \mathbb{Q}(\zeta)^+$. Como cada fator do produto acima é real, segue que $\pm \zeta^e$ deve ser real, e assim, devem ser apenas ± 1 , o que prova o item 1. $\square$

É possível mostrar que as unidades ciclotômicas são de índice finito no grupo das unidades completo. Assim, será suficiente trabalhar no subcorpo real. A seguir, apresentamos alguns resultados de unidades ciclotômicas que serão úteis, entretanto, as demonstrações desses resultados usam uma teoria que não foi abordada em nenhum momento neste contexto, e assim, não serão feitas e podem ser encontradas em [7] (Teoremas 12.4.1 e 12.4.2) ou em [15] (Teoremas 8.2 e 8.3). O primeiro apresenta o caso mais simples, o de potência de primos.

Teorema 5.4.5. *Seja $n = p^m$, com p um primo e $m \geq 1$. As unidades ciclotômicas $C_{\mathbb{K}^+} = C_{p^m}^+$ de $\mathcal{O}_{\mathbb{K}^+}$, com $\mathbb{K}^+ = \mathbb{Q}(\zeta + \zeta^{-1})$, são de índice finito no grupo $E = E_{p^m}^+$ e*

$$h = h_{p^m}^+ = [E : C_{\mathbb{K}^+}],$$

onde h é o número de classes de $\mathbb{K}^+$.

Observação 5.4.6. Se n não é uma potência de primos, então nem toda unidade ciclotômica é um produto de raízes da unidade e números da forma $\left(\frac{1 - \zeta_n^a}{1 - \zeta_n} \right)$, com $\text{mdc}(a, n) = 1$, ou seja, cada um desses produtos é uma unidade real vezes uma raiz da unidade, enquanto a unidade ciclotômica $1 - C_n$ não é desta forma, conforme Corolário 5.3.11.

Apresentamos o caso mais geral, onde n é um número inteiro qualquer.

Teorema 5.4.7. *Sejam $n = p_1^{e_1} \dots p_s^{e_s}$, com p_i sendo primos distintos e $e_i \geq 1$, para $1 \leq i \leq s$, $\mathbb{K} = \mathbb{Q}(\zeta_n)$ e $\mathbb{K}^+ = \mathbb{Q}(\zeta + \zeta^{-1})$. Para cada conjunto I pertencente a $\Gamma = \{I \subset \{1, \dots, s\}\}$, seja $n_I = \prod_{i \in I} p_i^{e_i}$. Se a é um número inteiro tal que $1 < a < \frac{n}{2}$ e $\text{mdc}(a, n) = 1$, então os números*

$$\xi_a = \prod_{i \in I} \zeta_n^{\frac{n_I(1-a)}{2}} \left(\frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}} \right) \quad (5.7)$$

formam um conjunto de unidades multiplicativamente independentes de $\mathbb{K}^+$. Além disso, o subgrupo

$$C = \left\langle -1, \xi_a \mid 1 < a < \frac{n}{2}, \text{mdc}(a, n) = 1 \right\rangle,$$

tem índice não nulo em $\mathcal{O}_{K^+}^*$.

6 Reticulado logarítmico

Há uma importante relação entre empacotamento esférico e a Teoria de Códigos, que se explicita no fato de que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes. A partir desta percepção, passaram a associar o estudo dos códigos aos reticulados e surgiram várias famílias de reticulados.

Neste capítulo apresentamos os conceitos básicos sobre reticulados na Seção 6.1 e sobre empacotamento esférico e reticulado na Seção 6.2. Na Seção 6.3 apresentamos a definição de mínimo sucessivo. Nas Seções finais, 6.4 e 6.5, introduzimos o reticulado logarítmico e apresentamos seu raio de cobertura em um corpo ciclotômico.

6.1 Reticulados

Para darmos seguimento, dedicamos as primeiras seções para uma introdução à Teoria dos Reticulados, com o objetivo de introduzir os reticulados logarítmicos, objeto principal de estudo desse trabalho.

Definição 6.1.1. Seja $\mathcal{B} = \{v_1, v_2, \dots, v_m\} \subset \mathbb{R}^n$ uma coleção de $m \leq n$ vetores linearmente independentes. O conjunto

$$\Lambda(\mathcal{B}) = \left\{ \sum_{i=1}^m a_i u_i \mid a_i \in \mathbb{Z}, 1 \leq i \leq m \right\}, \quad (6.1)$$

é chamado **reticulado m -dimensional** em $\mathbb{R}^n$, com base $\mathcal{B}$. Se $m = n$, dizemos que $\Lambda(\mathcal{B})$ é um **reticulado de posto completo**.

Como trabalhamos apenas com reticulados completos, por simplicidade, chamamos apenas de reticulado, sem o risco de confusão.

Observação 6.1.2. Podemos reescrever a definição de reticulados tomando $\mathbb{R} = \mathbb{K}$, $\mathbb{R}^n = V$ um espaço vetorial e $A = \mathbb{Z}$.

Ainda, outra maneira de ver os reticulados é como $\mathbb{Z}$ -módulos livres de posto finito contidos no $\mathbb{R}^n$, onde a base $\mathcal{B} = \{v_1, \dots, v_n\}$ é linearmente independente sobre $\mathbb{R}$. Assim,

$$\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_n. \quad (6.2)$$

Como um módulo é um grupo abeliano aditivo, segue que Λ é um grupo abeliano aditivo no espaço euclidiano. Em particular, a soma ou a diferença de quaisquer dois vetores do reticulado ainda é um vetor do reticulado.

Exemplo 6.1.3. Um reticulado bastante conhecido é $\Lambda = \mathbb{Z}^2$ no $\mathbb{R}^2$, com a base canônica dada por $\{(1, 0), (0, 1)\}$. Este reticulado é dado por

$$\Lambda = \{a(1, 0) + b(0, 1) \mid a, b \in \mathbb{Z}\}.$$

Geometricamente, obtemos a seguinte representação.

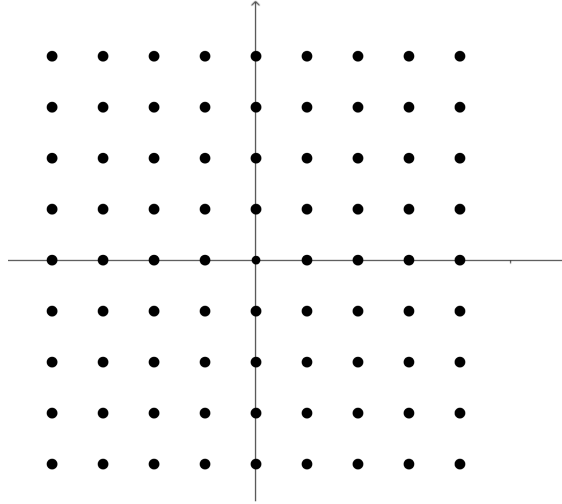


Figura 6.1: Reticulado $\mathbb{Z}^2$.

Exemplo 6.1.4. O Exemplo 6.1.3 pode ser expandido, e assim, obtemos o reticulado $\Lambda = \mathbb{Z}^n$ no $\mathbb{R}^n$, também com a base canônica $\mathcal{B} = \{e_i = (0, \dots, 0, \underbrace{1}_{i\text{-ésima coordenada}}, 0, \dots, 0) \mid 1 \leq i \leq n\}$.

Observação 6.1.5. Um mesmo reticulado pode ter mais do que uma base. Para que isso seja possível, a matriz de mudança da base $\mathcal{B}$ para $\mathcal{C}$ deve ser inversível. Em outras palavras, o reticulado Λ terá duas bases, $\mathcal{B}$ e $\mathcal{C}$, se $M_{\mathcal{B}\mathcal{C}}$ tem entradas inteiras e determinante ± 1 .

Proposição 6.1.6. *Seja Λ um reticulado de base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$. O conjunto $\mathcal{C} = \{u_1, u_2, \dots, u_n\} \subseteq \Lambda$ de vetores linearmente independentes sobre $\mathbb{R}$ tais que*

$$u_i = \sum_{j=1}^n a_{ij} v_j, \text{ com } a_{ij} \in \mathbb{Z},$$

é base de Λ se, e somente se, $\det(a_{ij}) = \pm 1$.

Demonstração. Por hipótese, segue que

$$u_i = \sum_{j=1}^n a_{ij} v_j, \quad a_{ij} \in \mathbb{Z},$$

isto é, os elementos de $\mathcal{C}$ podem ser escritos como combinação linear de elementos de $\mathcal{B}$. Escrevendo na forma matricial, segue que

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}.$$

Assim, $\mathcal{C}$ é uma base de Λ se, e somente se, $\det(a_{ij}) = \pm 1$, ou seja, a matriz mudança de base é inversível. $\square$

A seguir, provaremos que o reticulado é um subconjunto discreto do $\mathbb{R}^n$. Para isso, relembremos o que é um subgrupo discreto.

Definição 6.1.7. Seja H um subgrupo do $\mathbb{R}^n$. Dizemos que H é um subgrupo **discreto** se para qualquer conjunto compacto $K \subset \mathbb{R}^n$, $H \cap K$ é finito.

Proposição 6.1.8. O conjunto dos pontos de um reticulado $\Lambda \subseteq \mathbb{R}^n$ é discreto.

Demonstração. Para mostrarmos que é discreto, devemos provar que os pontos de Λ não são de acumulação. Para isso, considere $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ uma base de Λ . Considere o seguinte sistema linear:

$$\begin{cases} \langle x, v_1 \rangle = 0 \\ \langle x, v_2 \rangle = 0 \\ \vdots \\ \langle x, v_n \rangle = 0, \end{cases} \quad \text{com } x \neq 1.$$

Esse sistema possui $(n - 1)$ equações e n incógnitas, e assim, possui infinitas soluções. Logo, esse sistema deve possuir ao menos uma solução x não-nula. Se $\langle x, v_1 \rangle = 0$, então x é ortogonal a todos os vetores de $\mathcal{B}$, o que é impossível uma vez que $x \neq 0$. Portanto, $\langle x, v_1 \rangle \neq 0$. Assim, considere $u_1 = \frac{x}{\langle x, v_1 \rangle}$ que satisfaz $\langle u_1, v_1 \rangle = 1$ e é ortogonal a cada vetor restante $v_2, \dots, v_n$. Do mesmo modo, considere $u_i = \frac{x}{\langle x, v_i \rangle}$, para cada $i = 1, \dots, n$.

Analogamente, $\langle u_i, v_j \rangle = 0$ e $\langle u_i, v_i \rangle = 1$, para todo $i \neq j$. Considere $z = \sum_{i=1}^n a_i v_i \in \Lambda$, $a_i \in \mathbb{Z}$, tal que z pertence a uma bola de raio r . Logo,

$$u_i = \langle z, u_i \rangle.$$

Pela desigualdade de Cauchy-Schwarz, segue que

$$\|a_i\| = \|\langle z, u_i \rangle\| \leq \|z\| \cdot \|u_i\| < r \cdot \|u_i\|.$$

Como $r \cdot \|u_i\|$ não depende de z , segue que existe um número finito de possibilidades para a_i . Assim, o conjunto de todos os $z \in \Lambda$ tal que $\|z\| < r$ é finito. Em outras palavras, mostramos que a intersecção de Λ com qualquer compacto de $\mathbb{R}^n$ é finito. Portanto, os pontos de Λ não são pontos de acumulação e concluímos que é discreto. $\square$

Proposição 6.1.9. Se $H \subset \mathbb{R}^n$ é um subgrupo aditivo discreto, então H é um reticulado.

Demonstração. Sejam $v_1, \dots, v_m$ o conjunto maximal dos $\mathbb{R}$ -elementos independentes de H . Assim, todo elemento de H pode ser escrito da forma

$$h = r_1 v_1 + \dots + r_m v_m, \text{ onde } r_i \in \mathbb{R}.$$

Note que H contém o reticulado dado por

$$\Lambda = \mathbb{Z}v_1 + \dots + \mathbb{Z}v_m.$$

Seja $K = \{c_1 v_1 + \dots + c_m v_m \mid 0 \leq c_i < 1\}$ um conjunto compacto. Note que todo elemento $h \in H$ pode ser escrito como

$$\gamma + k, \gamma \in \Lambda + k \in K \cap H.$$

Mas, $K \cap H = \{h_1, \dots, h_r\}$ é um conjunto finito. Logo, Λ é um subgrupo de índice finito em H . Dessa forma, existe d inteiro positivo tal que $dH \subset \Lambda$. Portanto, $H \subset \frac{1}{d}\Lambda$, onde $\frac{1}{d}\Lambda$ é um $\mathbb{Z}$ -módulo livre de posto finito m . Como H é um subconjunto de $\frac{1}{d}\Lambda$, que tem posto m , segue que H é um $\mathbb{Z}$ -módulo livre e tem posto $l \leq m$. Denotamos por $w_1, \dots, w_l$ seus geradores. Agora, $v_1, \dots, v_m \in H$ e o $\mathbb{R}$ -módulo gerado por estes elementos tem dimensão m e está contido no $\mathbb{R}$ -módulo gerado por $w_1, \dots, w_l$. Portanto, $m = l$, ou seja, $w_1, \dots, w_m$ são linearmente independentes sobre $\mathbb{R}$. Logo, H é um reticulado. $\square$

Corolário 6.1.10. *Seja Λ um subgrupo aditivo de $\mathbb{R}^n$. O conjunto Λ é um reticulado se, e somente se, Λ é um subgrupo discreto do $\mathbb{R}^n$.*

Demonstração. Segue direto da aplicação das Proposições 6.1.8 e 6.1.9. $\square$

Exemplo 6.1.11. Como havíamos citado, $\mathbb{Z}^n$ é um reticulado de $\mathbb{R}^n$, uma vez que forma um subgrupo discreto aditivo de $\mathbb{R}^n$. Mas, $\mathbb{Q}^n \subseteq \mathbb{R}^n$, apesar de ser subgrupo aditivo, não é reticulado pois não é discreto.

Definição 6.1.12. Seja Λ um reticulado de $\mathbb{R}^n$ com base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$. O conjunto dado por

$$\mathcal{P} = \left\{ x = \sum_{i=1}^n \lambda_i v_i \mid 0 \leq \lambda_i < 1 \right\},$$

é chamado **região fundamental** do reticulado.

Exemplo 6.1.13. A região fundamental do reticulado $\mathbb{Z}^2$ mostrado no Exemplo 6.1.3 é dada pelo polígono com vértices $(0, 0)$, $(1, 0)$, $(0, 1)$ e $(1, 1)$.

A região fundamental $\mathcal{P}$ de um reticulado Λ pode ser transladada pelo espaço $\mathbb{R}^n$. Se a translação for feita pela adição de um elemento $l \in \Lambda$ não nulo, então a nova região não intercepta a região fundamental.

A seguir, apresentamos outras definições importantes no estudo dos reticulados.

Definição 6.1.14. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado com base $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$. Se cada v_i pode ser escrito em coordenadas reais de cada vetor da base $\mathcal{B}$, isto é, $v_i = (v_{i1}, v_{i2}, \dots, v_{in})$, onde $i = 1, \dots, n$, então a matriz

$$\mathcal{M} = [v_{ij}]_{1 \leq i, j \leq n} = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \dots & v_{nn} \end{bmatrix}$$

é chamada **matriz geradora** de Λ .

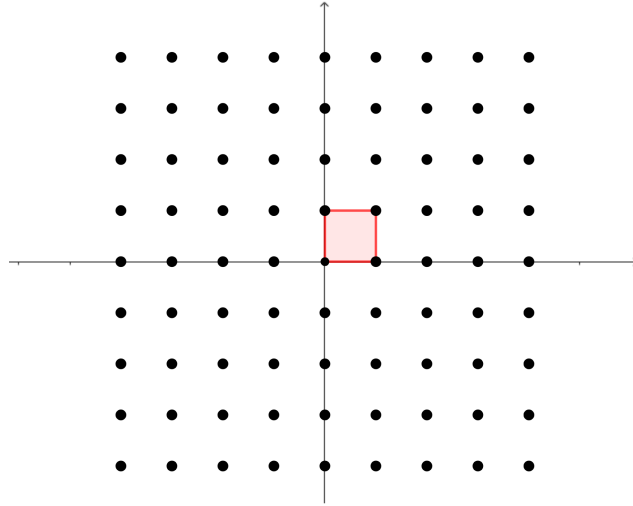


Figura 6.2: Região fundamental do reticulado $\mathbb{Z}^2$

Note que, com as mesmas hipóteses da Definição 6.1.1, podemos descrever o reticulado como sendo

$$\Lambda = \{\lambda \mathcal{M} \mid \lambda \in \mathbb{Z}^n\}.$$

Definição 6.1.15. Seja Λ um reticulado com região fundamental $\mathcal{P}$. O **volume do reticulado** Λ é definido por

$$\text{vol}(\Lambda) = \text{vol}(\mathcal{P}) = |\det(\mathcal{M})|.$$

Observação 6.1.16. Também é possível calcular o volume do reticulado utilizando μ (medida de Lebesgue em $\mathbb{R}^n$), onde $\text{vol}(\mathcal{P}) = \mu(\mathcal{P}) = \int_{\mathcal{P}} d\mu$.

Proposição 6.1.17. O volume de um reticulado $\Lambda \subset \mathbb{R}^n$ não depende da escolha de sua base.

Demonstração. Considere duas bases do reticulado Λ . Digamos $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ e $\mathcal{C} = \{u_1, u_2, \dots, u_n\}$. Como ambas são base, pela Proposição 6.1.6, segue que a matriz mudança de base de $\mathcal{B}$ para $\mathcal{C}$, $M_{\mathcal{BC}}$, tem determinante ± 1 , isto é,

$$\det(M_{\mathcal{BC}}) = \pm 1.$$

Seja $\mathcal{M}$ a matriz geradora de Λ formada pelas coordenadas dos vetores de $\mathcal{B}$ e $\mathcal{M}'$ a matriz formada pelas coordenadas dos vetores relacionados a $\mathcal{C}$. Assim,

$$\begin{aligned} \mathcal{M}' &= M_{\mathcal{BC}} \mathcal{M} \\ \Rightarrow \det(\mathcal{M}') &= \det(M_{\mathcal{BC}} \mathcal{M}) \\ \Rightarrow |\det(\mathcal{M}')| &= |\det(M_{\mathcal{BC}} \mathcal{M})| \\ \Rightarrow |\det(\mathcal{M}')| &= \underbrace{|\det(M_{\mathcal{BC}})|}_1 |\det(\mathcal{M})| \\ \Rightarrow |\det(\mathcal{M}')| &= |\det(\mathcal{M})|. \end{aligned}$$

Pela Definição 6.1.15, segue que o volume do reticulado é calculado justamente pelo módulo do determinante da matriz geradora de uma base de Λ , ou seja, independente da base escolhida, o volume do reticulado não se altera. $\square$

Definição 6.1.18. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado cuja matriz geradora é dada por $\mathcal{M}$. A **matriz de Gram** associada a $\mathcal{M}$ é dada por

$$G = \mathcal{M}^T \mathcal{M}.$$

Note que a matriz de Gram é sempre uma matriz simétrica, mas ela não é fixa para o reticulado, podendo se alterar dependendo da base ou da matriz geradora.

Exemplo 6.1.19. Considere o reticulado $\Lambda = \mathbb{Z}^2$ gerado por $\mathcal{B} = \{(n, n+1), (-n-1, n) \mid n \in \mathbb{Z}\}$. Outra base de Λ é dada por $\mathcal{C} = \{(n, n+1), (-1, 2n+1) \mid n \in \mathbb{Z}\}$. As matrizes geradoras de $\mathcal{B}$ e $\mathcal{C}$ são dadas, respectivamente, por

$$\mathcal{M} = \begin{bmatrix} n & -n-1 \\ n+1 & n \end{bmatrix} \text{ e } \mathcal{M}' = \begin{bmatrix} n & -1 \\ n+1 & 2n+1 \end{bmatrix}.$$

Quando calculamos as matrizes de Gram de cada uma dessas matrizes geradoras, respectivamente, obtemos

$$G' = \mathcal{M}^T \mathcal{M} = \begin{bmatrix} n & n+1 \\ -n-1 & n \end{bmatrix} \cdot \begin{bmatrix} n & -n-1 \\ 1 & n \end{bmatrix} = \begin{bmatrix} 2n^2 + 2n + 1 & 0 \\ 0 & 2n^2 + 2n + 1 \end{bmatrix} \text{ e}$$

$$G' = \mathcal{M}^T \mathcal{M} = \begin{bmatrix} n & n+1 \\ -1 & 2n+1 \end{bmatrix} \cdot \begin{bmatrix} n & -1 \\ n+1 & 2n+1 \end{bmatrix} = \begin{bmatrix} 2n^2 + 2n + 1 & 2n^2 + 2n + 1 \\ 2n^2 + 2n + 1 & 4n^2 + 4n + 2 \end{bmatrix}.$$

Apesar das matrizes de Gram de um reticulado serem distintas, veremos a seguir que o determinante delas é o mesmo, e esse só depende do reticulado.

Proposição 6.1.20. Sejam $\Lambda \subset \mathbb{R}^n$ um reticulado de base $\mathcal{B}$ e matriz de Gram G . Se $\mathcal{C}$ for outra base de Λ , então $\det(G) = \det(G')$, onde G' é a matriz de Gram de Λ com relação a base $\mathcal{C}$.

Demonstração. Considere $A = M_{\mathcal{BC}}$ a matriz mudança de base de $\mathcal{B}$ para $\mathcal{C}$. A prova segue direto do fato de que $\det(A) = \pm 1$. Neste caso, $\mathcal{M}' = A\mathcal{M}$. Assim,

$$\begin{aligned} \det(G') &= \det((\mathcal{M}')^T \mathcal{M}') = \det(\mathcal{M}^T A^T A \mathcal{M}) \\ &= \det(\mathcal{M}') \det(A^T) \det(A) \det(\mathcal{M}) \\ &= \det(\mathcal{M}^T \mathcal{M}) = \det(G) \end{aligned}$$

Portanto, $\det(G') = \det(G)$. □

Exemplo 6.1.21. No Exemplo 6.1.19, ambas matrizes de Gram tem determinante igual a $(2n^2 + 2n + 1)^2$.

Definição 6.1.22. Se $\Lambda \subset \mathbb{R}^n$ é um reticulado, então o **determinante do reticulado** Λ é definido pelo determinante da matriz de Gram de Λ . Assim,

$$\det(\Lambda) = \det(G) = (\det(\mathcal{M}))^2 = (\text{vol}(\mathcal{P}))^2.$$

Definição 6.1.23. Se $\Lambda \subset \mathbb{R}^n$ é um reticulado e Λ' é um subgrupo aditivo contido em Λ , dizemos que Λ' é um **sub-reticulado** de Λ . Quando for finito, o índice do subgrupo Λ' em $[\Lambda : \Lambda']$, é dado pelo número de elementos do quociente Λ/Λ' e pode ser calculado pela razão $[\Lambda : \Lambda'] = \frac{\text{vol}(\Lambda')}{\text{vol}(\Lambda)}$.

6.2 Empacotamento esférico no $\mathbb{R}^n$

Um problema clássico da geometria é o do empacotamento esférico. O empacotamento esférico consiste em encontrar a melhor maneira de distribuir esferas idênticas maciças, de modo que preencham o máximo de espaço possível, em termos de densidade.

Esse problema tem diversas aplicações como a Teoria da Informação, Otimização, Física, Química, Biologia, Medicina, etc. Entretanto, podemos exemplificá-lo de maneira muito simples, como no seguinte exemplo: *Sem amontoar uma em cima da outra, quantas moedas de 1 real cabem em uma quadra de vôlei?*

Uma maneira natural de responder esse problema seria considerar o diâmetro da moeda, que é de 27mm, e a medida da quadra de vôlei padrão, que tem 18×9m. Assim, calcular a quantidade de fileiras no sentido do comprimento e repetir o processo no sentido da largura. Multiplicando esses valores, obter a quantidade de moedas. Numericamente,

$$\frac{18m}{27mm} \approx 666 \text{ moedas e } \frac{9m}{27mm} \approx 333 \text{ moedas.}$$

Isto é, o número total de moedas que cabem nesse espaço seria $333 \times 666 \approx 221778$ moedas. Entretanto, se fosse feito isso, estaria apenas preenchendo no máximo 78% de todo espaço livre da quadra, pois ao colocar uma circunferência do lado da outra, sobra um espaço que não é preenchido.

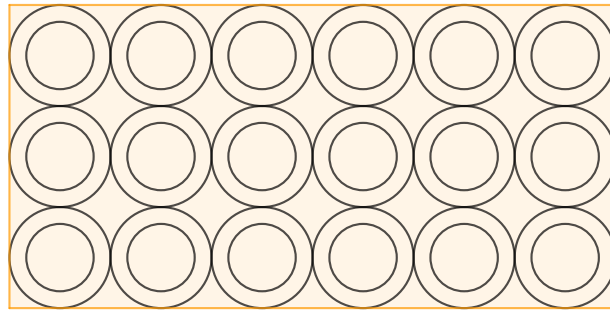


Figura 6.3: Representação das moedas colocadas por fileira

Mostraremos nesta seção que nem sempre a maneira mais natural de resolver esse problema é a melhor. Note que se substituir a moeda por círculo e a quadra de vôlei pelo espaço $\mathbb{R}^2$, vemos que é um problema de empacotamento esférico. Veremos que a melhor forma de resolvê-lo, seria colocar os círculos inscritos em hexágonos. Dessa maneira, é possível ocupar um pouco mais de 90% da área total.

Esse problema pode ser expandido, como no seguinte exemplo: *Quantas bolas de vinil cabem em um galpão?* Intuitivamente nota-se que o problema é parecido com o anterior, mas a diferença é que ao invés de círculos (moedas) e áreas, o trabalho é determinar quantas esferas (bolas) ocupam um determinado volume do espaço.

Resumindo, no caso de duas dimensões, obtemos o plano e consideramos círculos e suas áreas; em três dimensões, o espaço e fazemos a análise com esferas e volumes. Mas, sem perder a ideia de empacotamento, podemos estender para espaços de dimensões maiores.

Algumas perguntas naturais relacionadas a esse problema são:

1. Dada uma dimensão, qual a maior densidade possível que se podem alcançar empacotando o espaço com esferas idênticas que apenas se tangenciam?

2. Neste caso, qual é a disposição e raio dessas esferas?

Em outras palavras, como é possível resolver esse problema de preencher o espaço utilizando esferas maciças tangentes idênticas deixando o menor espaço possível sem preenchimento? Estas perguntas não tem respostas para todas as dimensões. Para ter a resposta em algumas dimensões, iremos transferir esse problema para o conceito de reticulados, onde o centro de cada esfera vai formar o subgrupo discreto que define o reticulado.

Definição 6.2.1. Um **empacotamento esférico** em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio ρ no $\mathbb{R}^n$ de forma que a interseção entre quaisquer duas esferas tenha no máximo um ponto.

Definição 6.2.2. Um **empacotamento reticulado** é um empacotamento esférico em que o conjunto dos centros das esferas formam um reticulado Λ no $\mathbb{R}^n$.

Pelas Definições 6.2.1 e 6.2.2, vimos que podemos descrever um empacotamento esférico apenas conhecendo o centro e o raio das esferas.

Definição 6.2.3. A **densidade de empacotamento** do reticulado $\Lambda \in \mathbb{R}^n$ é a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

Como queremos que as esferas cubram o maior espaço possível, segue que faz sentido estudar empacotamentos associados a um reticulado Λ em que as esferas tenham raio máximo. Para determinarmos esse raio, como o reticulado Λ é um conjunto discreto do $\mathbb{R}^n$, então fixado $k > 0$, obtemos a interseção de um conjunto compacto $K = \{x \in \mathbb{R}^n; |x| \leq k\}$ com Λ sendo finito. Assim, podemos definir o seguinte número

$$\Lambda_{\min} = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}.$$

Definição 6.2.4. Sejam $\Lambda \subseteq \mathbb{R}^n$ um reticulado e $\Lambda_{\min} = \min\{|\lambda|; \lambda \in \Lambda, \lambda \neq 0\}$. Chamamos de **norma mínima** de Λ , o número

$$N_{\min} = (\Lambda_{\min})^2.$$

Tendo isso em vista, o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento é $\rho = \frac{\Lambda_{\min}}{2}$. Observe que se o empacotamento que estamos analisando é reticulado, então podemos estender para o plano a análise da proporção ocupada pelas esferas na região fundamental. Dessa forma, conseguimos obter diretamente como encontrar a densidade de empacotamento.

Definição 6.2.5. A **densidade de empacotamento associada a um reticulado** $\Lambda \subset \mathbb{R}^n$ é dada por

$$\Delta(\Lambda) = \frac{\text{Volume da região coberta por uma esfera}}{\text{Volume da região fundamental}} = \frac{\text{vol}(B(0, \rho))}{\text{vol}(\Lambda)} = \frac{\text{vol}(B_n(1))\rho^n}{\text{vol}(\Lambda)},$$

em que $B(0, \rho)$ denota a esfera de centro na origem e raio ρ .

Observe que $\text{vol}(\Lambda) = \sqrt{\det(\Lambda)}$. Assim, podemos substituir esse valor direto na fórmula da densidade de empacotamento. Além disso, como o valor de $\text{vol}(B_n(1))$ é um valor fixo em cada dimensão n , podemos concluir que para maximizar o cálculo da densidade de um empacotamento reticulado associado a Λ , devemos maximizar o seguinte valor de

$$\frac{\rho^n}{\text{vol}(\Lambda)} = \frac{\rho^n}{\sqrt{\det(\Lambda)}}.$$

Definição 6.2.6. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. A **densidade de centro** de Λ é dada por

$$\delta(\Lambda) = \frac{\rho^n}{\text{vol}(\Lambda)} = \frac{\rho^n}{\sqrt{\det(\Lambda)}},$$

em que ρ é o raio de empacotamento de Λ .

A seguir, apresentamos alguns exemplos de empacotamentos esféricos e empacotamentos reticulados.

Exemplo 6.2.7. Para a dimensão $n = 1$, a melhor distribuição das "esferas" são dadas por intervalos na reta, centradas em números inteiros e de raio 0,5. Observe os intervalos cobrem a reta real toda. Assim, a densidade máxima de empacotamento em $\mathbb{R}$ é exatamente 1.

Exemplo 6.2.8. Para a dimensão $n = 2$, a melhor densidade possível é dada por $\frac{\pi}{12} \approx 0,907$. Para atingir essa densidade, as esferas (círculos no $\mathbb{R}^2$), estão inscritas em um hexágono e centradas no reticulado que tem matriz geradora dada por $\mathcal{M} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$, isto é, o reticulado é gerado pelos vetores $(1, 0)$ e $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$.

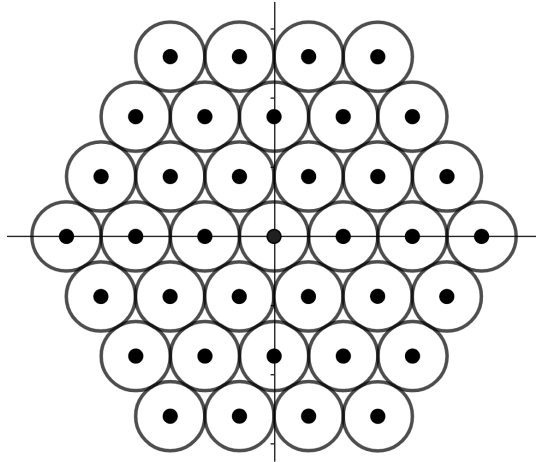


Figura 6.4: Cobertura esférica feita com o reticulado hexagonal

Este reticulado é chamado *reticulado hexagonal* e a escolha do hexágono é devido a este ser o polígono com mais lados que pavimenta o plano. Observe que a matriz de Gram de Λ é dada por

$$G = \mathcal{M}^T \mathcal{M} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix} = \begin{pmatrix} \frac{5}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{3}{4} \end{pmatrix} \approx \begin{pmatrix} 1.25 & 0.433013 \\ 0.433013 & 0.75 \end{pmatrix}.$$

Ainda, esse reticulado tem região fundamental dada pelo paralelogramo de vértices $(0, 0)$, $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, $\left(\frac{3}{2}, \frac{\sqrt{3}}{2}\right)$ e $(1, 0)$. A área desse paralelogramo é $\frac{\sqrt{3}}{2}$ e coincide com o a do volume num espaço n -dimensional.

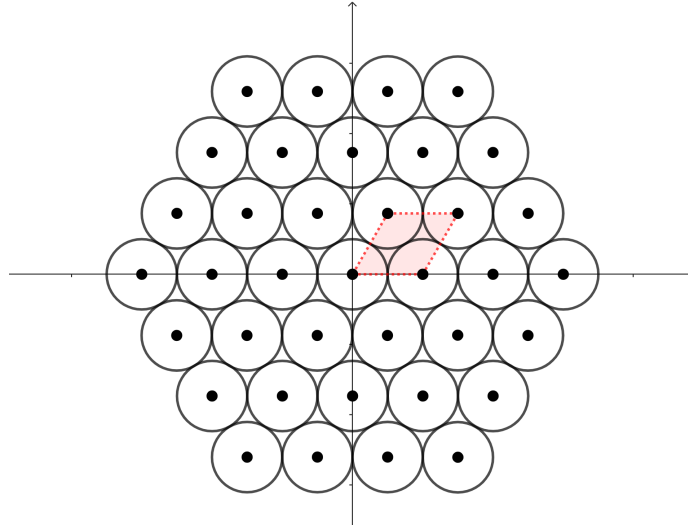


Figura 6.5: Região fundamental do reticulado hexagonal

Seja $\rho = \frac{\Lambda_{\min}}{2} = \frac{1}{2}$. Note que com esse raio, quaisquer duas esferas no plano (neste caso, círculos) tem apenas um ou nenhum ponto de interseção. Por fim, a densidade de empacotamento relacionada a Λ é

$$\Delta(\Lambda) = \frac{\rho^n \cdot \overbrace{\text{vol}(B(0,1))}^{\pi}}{\text{vol}(\Lambda)} = \frac{\left(\frac{1}{2}\right)^2 \pi}{\left(\frac{\sqrt{2}}{2}\right)} = \frac{\pi}{2\sqrt{3}} \approx 0,9069...$$

Exemplo 6.2.9. Se $\Lambda \in \mathbb{Z}^2$ com base $\mathcal{B} = \{(1,0), (0,1)\}$, então $\rho = \frac{1}{2}$ e $\text{vol}(B(0,1)) = \pi \cdot 1 = \pi$ e o volume do reticulado, pela Definição 6.1.22, é dado por

$$\text{vol}(\Lambda) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 \cdot 1 = 1.$$

A densidade de empacotamento é dada por

$$\Delta(\Lambda) = \text{vol}(B(0,1)) \cdot \frac{\rho^2}{\text{vol}(\Lambda)} = \pi \cdot \frac{\left(\frac{1}{2}\right)^2}{1} = \frac{\pi}{4}$$

e a densidade de centro é dada por

$$\delta(\Lambda) = \frac{\rho^2}{\text{vol}(\Lambda)} = \frac{1}{4}.$$

Exemplo 6.2.10. No caso das bolas de vinil no galpão, estamos considerando a dimensão $n = 3$. O reticulado que origina esse empacotamento é um subconjunto do $\mathbb{Z}^3$ dado por

$$\Lambda = \{(x_1, x_2, x_3) \in \mathbb{Z}^3 \mid x_1 + x_2 + x_3 = 2k, k \in \mathbb{Z}\}.$$

Uma possibilidade de base para este reticulado é dada por $\mathcal{B} = \{(-1, -1, 0), (1, -1, 0), (0, 1, -1)\}$. A partir disso, segue que

$$\begin{aligned} \rho &= \frac{\Lambda_{\min}}{2} = \frac{\sqrt{2}}{2} \quad (\text{raio de empacotamento}) \\ \delta(\Lambda) &= \frac{\sqrt{2}}{8\pi} \approx 0,1767... \quad (\text{densidade de centro}) \\ \Delta(\Lambda) &= \frac{\pi}{\sqrt{18}} \approx 0,741... \quad (\text{densidade de empacotamento}). \end{aligned}$$

Dessa forma, o espaço $\mathbb{R}^3$ pode ser preenchido no máximo 74,1%. Este reticulado é conhecido como *fcc* (*face - centered - cubic*) e foi provado por Gauss (1831) que este é o melhor empacotamento reticulado para esta dimensão.

Ainda sobre o problema da cobertura esférica, faremos uma última definição que será útil.

Definição 6.2.11. Sejam Λ um reticulado em $\mathbb{R}^n$ e H um subespaço de $\mathbb{R}^n$ gerado por Λ . Chamamos de **raio de cobertura** de Λ o valor

$$\mu(\Lambda) = \max_{x \in H} \min_{u \in \Lambda} |x - u|.$$

A interpretação geométrica do raio de cobertura $\mu(\Lambda)$ se dá pelo menor raio r tal que $\Lambda + B_n(r)$ cobre o subespaço H .

6.3 Mínimos sucessivos de um reticulado

Considere um reticulado Λ em $\mathbb{R}^n$, com $n \geq 2$. Como definido em 6.2.4, $N_{\min}(\Lambda)$ é a norma mínima do reticulado, sendo o mínimo entre as normas euclidianas de todos os seus vetores não nulos.

Definição 6.3.1. Os **vetores mínimos** de um reticulado $\Lambda \subset \mathbb{R}^n$ são os vetores $x \in \Lambda - 0$ com norma igual à norma mínima do reticulado. O conjunto de todos os vetores mínimos é denotado por $S(\Lambda)$ e é dado por

$$S(\Lambda) = \{x \in \Lambda \mid |x| = N_{\min}(\Lambda)\}.$$

Definição 6.3.2. O número de elementos do conjunto $S(\Lambda)$ é chamado de **número de contato** de Λ .

Definição 6.3.3. Seja $\Lambda \subset \mathbb{R}^n$ um reticulado. Chamamos de **k -ésimo mínimo sucessivo** de Λ o valor $\lambda_k(\Lambda)$ correspondente ao menor raio r tal que a bola centrada na origem de $\mathbb{R}^n$ com raio r contém k vetores linearmente independentes pertencentes a Λ , isto é,

$$\lambda_k(\Lambda) = \min\{r \mid B_n(0, r) \supset k \text{ vetores L.I.}, k \in \Lambda\}.$$

Outra interpretação do mínimo sucessivo $\lambda_k(\Lambda)$ é o menor valor real $r > 0$ tal que o reticulado Λ possui k vetores linearmente independentes com norma euclidiana menor ou igual a r . Consequentemente, obtemos a seguinte desigualdade:

$$\lambda_1(\Lambda) \leq \lambda_2(\Lambda) \leq \dots \leq \lambda_n(\Lambda).$$

Em particular, para $k = 1$, $\lambda_1(\Lambda)$ é uma outra maneira de chamar a norma mínima $N_{\min}(\Lambda)$ do reticulado Λ em $\mathbb{R}^n$. Neste caso, $\lambda_1(\Lambda)$ é chamado de *primeiro mínimo sucessivo* de Λ .

Observação 6.3.4. Neste contexto, não há risco de confusão do reticulado que estamos trabalhando. Assim, por simplicidade, denotamos o mínimo sucessivo $\lambda_k(\Lambda)$ apenas por λ_k .

Definição 6.3.5. O invariante de Hermite de um reticulado $\Lambda \subset \mathbb{R}^n$ é definido por

$$\gamma(\Lambda) = \frac{N_{\min}(\Lambda)^2}{\det(\Lambda)^{\frac{1}{n}}}$$

e a constante de Hermite de dimensão n é definida por

$$\gamma_n = \sup_{\Lambda \subset \mathbb{R}^n} \gamma(\Lambda).$$

Definição 6.3.6. Um reticulado Λ tal que

$$\gamma(\Lambda) = \gamma_n,$$

é chamado **reticulado crítico** em dimensão n .

Note que, podemos reescrever a densidade de centro $\delta(\Lambda)$, definida em 6.2.6, como

$$\delta(\Lambda) = 2^{-n} \gamma(\Lambda)^{\frac{n}{2}}.$$

Teorema 6.3.7. [19] Se Λ é um reticulado n -dimensional, então

$$\frac{\lambda_n(\Lambda)}{n} \leq \mu(\Lambda) \leq \frac{\sqrt{n\lambda(\Lambda)}}{2}.$$

6.4 Reticulado logarítmico

O grupo das unidade do anel de inteiros de um corpo numérico é finitamente gerado, pelo *Teorema das Unidades de Dirichlet*, que fornece em termos abstratos a caracterização desse grupo. O reticulado logarítmico é obtido através de um mergulho logarítmico, que também definimos nesta seção. Veremos que este reticulado não tem posto completo no espaço euclidiano de dimensão igual ao grau do corpo, um fato diferente dos reticulados que vínhamos abordado nas seções anteriores. O objetivo desse estudo é por sua aplicação, uma vez que os reticulados logarítmicos tem sido aplicados tanto em códigos quanto em criptografia.

A seguir, considere $\mathbb{K}$ um corpo de números algébrico de grau $n \leq 2$. Sejam $\sigma_1, \sigma_2, \dots, \sigma_n$ os monomorfismos de $\mathbb{K} \rightarrow \mathbb{C}$, onde $\sigma_1, \dots, \sigma_r$ representam os monomorfismos reais e $\sigma_{r+1}, \dots, \sigma_{r+s}$, os monomorfismos complexos. Lembre que os monomorfismos complexos ocorrem em pares conjugados. Logo, $n = r + 2s$.

Definição 6.4.1. Seja $\mathbb{K}$ um corpo de números de grau $n = r + 2s$. Chamamos de **assinatura** de $\mathbb{K}$ o par (r, s) , onde r representa a quantidade de monomorfismos reais de $\mathbb{K}$ em $\mathbb{C}$ e s , a quantidade de monomorfismos complexos.

O conjunto dos n monomorfismos é dado por

$$\{\sigma_1, \dots, \sigma_r, \sigma_{r+1}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s-1}}, \dots, \overline{\sigma_{r+s}}\}.$$

Algumas vezes, denotamos esse conjunto por $\{\tau_1, \tau_2, \dots, \tau_n\}$, para facilitar a notação, quando for conveniente.

Seja $\phi : \mathbb{K} \rightarrow V$, onde $V = \mathbb{R}^r \times \mathbb{C}^s$ definida por

$$\phi(\alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_{r+s}(\alpha)).$$

Fixe uma base integral $\alpha_1, \alpha_2, \dots, \alpha_n$ de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim, pela Definição 2.5.7 e pelo Corolário 2.5.13, segue que $(\det(\tau_i(\alpha_i)))^2 = d(\mathbb{K}) \neq 0$. Além disso, os vetores $\phi(\alpha_1), \dots, \phi(\alpha_n)$ são $\mathbb{R}$ -linearmente independentes em V . Agora, um reticulado em V é, por definição, um subgrupo aditivo de V , que pode ser escrito na forma $\mathbb{Z}v_1 + \dots + \mathbb{Z}v_l$, onde $v_1, \dots, v_l$ são elementos $\mathbb{R}$ -linearmente independentes de V . Seja $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$. Assim, mostramos o seguinte resultado:

Teorema 6.4.2. *Se $\mathcal{O}_{\mathbb{K}}$ é um anel de inteiros de $\mathbb{K}$, então $\phi(\mathcal{O}_{\mathbb{K}})$ é um reticulado.*

A seguir, vamos definir uma aplicação λ que sai do subconjunto aberto $\mathbb{R}^r \times \mathbb{C}^s$ que consiste em todos os pontos cuja nenhuma coordenada é zero em $\mathbb{R}^{r+s}$.

Definição 6.4.3. Defina $\lambda : V \rightarrow \mathbb{R}^{r+s}$ dada por

$$\lambda(\alpha_1, \dots, \alpha_{r+s}) = (\log |\alpha_1|, \dots, \log |\alpha_r|, 2 \log |\alpha_{r+1}|, \dots, 2 \log |\alpha_{r+s}|).$$

Observe que a composição das funções ϕ e λ fornece uma aplicação de $\mathbb{K}$ em $\mathbb{R}^{r+s}$. Denotamos essa composição por Log e chamamos de mergulho logarítmico.

Definição 6.4.4. A função $Log : \mathbb{K}^* \rightarrow \mathbb{R}^{r+s}$ tal que, para todo $x \in \mathbb{K}^*$,

$$Log(x) = (\log |\sigma_1(x)|, \dots, \log |\sigma_r(x)|, 2 \log |\sigma_{r+1}(x)|, \dots, 2 \log |\sigma_{r+s}(x)|), \quad (6.3)$$

onde $\log$ denota a função logarítmica com base 10 em $\mathbb{R}$, é chamada de **mergulho logarítmico**.

Observação 6.4.5. Seja y um número complexo. A notação $|y|$ se refere à norma complexa, dada por $|y| = \sqrt{\mathcal{R}(y)^2 + \mathcal{F}(y)^2}$, onde $\mathcal{R}$ representa a parte real deste número e $\mathcal{F}$, a parte complexa.

Note que pela topologia, imagem inversa de compacto, é compacto. Logo, $\lambda^{-1}(\mathbb{K})$ é compacto quando $\mathbb{K}$ é um subconjunto compacto de $\mathbb{R}^{r+s}$. Lembre que uma das propriedades notáveis do logaritmo é que

$$\log(xy) = \log(x) + \log(y), \quad \text{para todo } x, y \in \mathbb{O}_{\mathbb{K}}^*.$$

Dessa forma, podemos concluir diretamente que o mergulho logarítmico é um homomorfismo do grupo multiplicativo $\mathbb{K}^* = \mathbb{K} - \{0\}$ de $\mathbb{K}$ no grupo aditivo $\mathbb{R}^{r+s}$. Agora, considere a restrição do homomorfismo Log ao grupo das unidade do anel de inteiros de $\mathbb{K}$, isto é, $U(\mathcal{O}_{\mathbb{K}}) = \mathcal{O}_{\mathbb{K}}^*$. Assim,

$$Log : \mathcal{O}_{\mathbb{K}}^* \rightarrow \mathbb{R}^{r+s}. \quad (6.4)$$

O núcleo deste homomorfismo é dado pelo grupo W , conjunto das raízes da unidade pertencentes a $\mathcal{O}_{\mathbb{K}}^*$.

Proposição 6.4.6. *O núcleo W de $Log : \mathcal{O}_{\mathbb{K}}^* \rightarrow \mathbb{R}^{r+s}$ é dado pelo conjunto de todas as raízes da unidade pertencentes a $\mathcal{O}_{\mathbb{K}}^*$.*

Demonstração. Queremos encontrar o conjunto W tal que $Log(W) = 0$. Note que

$$Log(\alpha) = 0 \Leftrightarrow |\sigma_i(\alpha)| = 1, \quad \text{para todo } i = 1, \dots, n.$$

Assim, note que o corpo de polinômios $\mathbb{P}$, dado por

$$\prod_i (r - \sigma_i(\alpha))$$

está em $\mathbb{Z}[t]$. Agora, observe que se $p(t)$ é um polinômio com todos os zeros em $\mathbb{C}$ tendo valor absoluto 1, então todos os zeros são raízes da unidade. Assim, $\sigma_i(\alpha)$ é uma raiz da unidade. Em particular, α também é uma unidade. Logo, o conjunto de todos os α forma o núcleo de Log , e portanto, obtemos o que queríamos. $\square$

Pelo Teorema 4.4.14, segue que W consiste em um grupo multiplicativo cíclico finito. Como $(-1) \in W$ e (-1) tem ordem par, segue que a ordem de W deve ser par.

Teorema 6.4.7. *$\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ é um reticulado.*

Demonstração. Se K é um compacto em $\mathbb{R}^{r+s}$, então $S = \lambda^{-1}(K \cap \text{Log}(\mathcal{O}_{\mathbb{K}}^*)) \subset \phi(\mathcal{O}_{\mathbb{K}})$. Além disso, S é finito, uma vez que $\phi(\mathcal{O}_{\mathbb{K}})$ é um reticulado pelo Teorema 6.4.2 e sabemos como é dada a aplicação λ . Logo, $K \cap \text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ é finito e, portanto, $\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ é discreto. Mas, observe que definimos Log como um homomorfismo do grupo multiplicativo $U(\mathbb{K}) = \mathbb{K}^*$ no grupo aditivo $\mathbb{R}^{r+s}$. Assim, pela Proposição 6.1.9, segue que $\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ é um reticulado. $\square$

Definição 6.4.8. O reticulado $\text{Log}(\mathcal{O}_{\mathbb{K}}^*) \subset \mathbb{R}^{r+s}$ é chamado **reticulado logarítmico** associado a $\mathbb{K}$.

Note que, até agora, não utilizamos o *Teorema das Unidades de Dirichlet*. Apesar disso, com a base teórica que criamos neste capítulo, poderíamos provar uma versão mais fraca dele.

Teorema 6.4.9. (Teorema das Unidades de Dirichlet fraco) *Se $\mathcal{O}_{\mathbb{K}}$ é o anel de inteiros de um corpo de números $\mathbb{K}$, então $U(\mathcal{O}_{\mathbb{K}}) = \mathcal{O}_{\mathbb{K}}^*$ é finitamente gerado.*

Demonstração. Considere $\mathcal{B} = \{v_1, v_2, \dots, v_l\}$ uma base para o reticulado $\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$. Sejam $u_1, \dots, u_l$ unidades com $\text{Log}(u_i) = v_i$. Se $u \in \mathcal{O}_{\mathbb{K}}^*$, então existem $c_i \in \mathbb{Z}$ tais que

$$\text{Log}(u) = c_1 v_1 + \dots + c_l v_l, \quad c_i \in \mathbb{Z}.$$

Agora, se $\zeta = u^{-1} u_1^{c_1} u_2^{c_2} \dots u_l^{c_l}$, então $\text{Log}(\zeta) = 0$, uma vez que o $\text{Ker}(\text{Log})$ é o grupo das raízes da unidade em $\mathcal{O}_{\mathbb{K}}$. Isso implicaria que ζ é uma raiz da unidade. Mas, o conjunto das raízes da unidade em $\mathbb{K}$ é finito. Logo, $u = \zeta^{-1} u_1^{c_1} \dots u_l^{c_l}$. Portanto, $\mathcal{O}_{\mathbb{K}}^*$ é finitamente gerado. $\square$

Observe que na versão original do *Teorema das unidades de Dirichlet* (4.2.1), apresentamos a prova de como as unidades são dadas. Entretanto, podemos reescrevê-lo da seguinte forma:

Teorema 6.4.10. *Seja $\mathbb{K}$ um corpo de números com assinatura (r, s) . Denotamos por W o grupo das raízes da unidade contidas em $\mathbb{K}$ e considere $l = r + s - 1$. Assim, o grupo aditivo $\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ é isomorfo $\mathbb{Z}^l$, ou seja, o grupo das unidades de $\mathbb{K}$ é isomorfo a $W \times \mathbb{Z}^l$.*

Como tínhamos visto, cada unidade u de $\mathcal{O}_{\mathbb{K}}^*$ pode ser escrita unicamente como

$$u = w u_1^{e_1} u_2^{e_2} \dots u_l^{e_l}, \quad w \in W, \quad e_i \in \mathbb{Z}, \quad (1 \leq i \leq l),$$

onde as unidades u_i formam o sistema de unidades fundamentais. Este teorema garante que o reticulado logarítmico $\Lambda = \text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ tem posto $l = r + s - 1$ em $\mathbb{R}^{r+s}$, isto é, não é completo.

Exemplo 6.4.11. Seja $\mathbb{K}$ um corpo quadrático imaginário. Neste caso, $r = 0$ e $s = 1$, e assim, $\mathbb{K}$ tem assinatura $(0, 1)$. Pelo *Teorema das Unidades de Dirichlet* (4.2.1), segue que o grupo das unidades de $\mathbb{K}$ é isomorfo ao conjunto das raízes da unidade, já que $l = r + s - 1 = 0$. Note que isso pode justificar que as unidades constituem um conjunto finito em cada um dos casos analisados na Seção 3.1.

Exemplo 6.4.12. Consideramos o corpo quadrático real $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, o qual tem assinatura $(2, 0)$. Já vimos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ pelo Teorema 2.4.8, uma vez que $3 \not\equiv 1 \pmod{4}$. Pelo Teorema 3.2.1, segue que o grupo das unidades é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}$. As raízes dos corpos quadráticos totalmente reais são dadas no Teorema 4.4.16. Como W não está em nenhum daqueles casos, segue que $W = \{\pm 1\}$. Pela Tabela 3.1, segue que $2 + \sqrt{3}$ é a unidade fundamental de $\mathbb{K} = \mathbb{Q}(\sqrt{3})$. Assim, pelo Teorema 3.6.2, segue que as outras unidades podem ser escritas como $\pm \eta^e$, $e \in \mathbb{Z}$.

$$a + b\sqrt{3} \in \mathcal{O}_{\mathbb{K}}^* \Leftrightarrow a + b\sqrt{3} = \pm(2 + \sqrt{3})^e, \quad e \in \mathbb{Z},$$

ou ainda,

$$\pm 1 = N_{\mathbb{K}}(a + b\sqrt{3}) = (a + b\sqrt{3})(a - b\sqrt{3}) = a^2 - 3b^2.$$

Logo, o mergulho logarítmico pode ser definido como $Log : \mathcal{O}_{\mathbb{K}}^* \rightarrow \mathbb{R}^2$, onde

$$\begin{aligned} Log(\pm(2 + \sqrt{3})^e) &= (\log |\sigma_1(\pm(2 + \sqrt{3})^e)|, \log |\sigma_2(\pm(2 + \sqrt{3})^e)|) \\ &= (e \log(2 + \sqrt{3}), e \log(2 - \sqrt{3})), \quad \text{onde } e \in \mathbb{Z}. \end{aligned}$$

Geometricamente, o reticulado $\Lambda = Log(\mathcal{O}_{\mathbb{K}}^*)$ de dimensão $n = r + s - 1 = 2 + 0 - 1 = 1$ em $\mathbb{R}^2$ é dado por

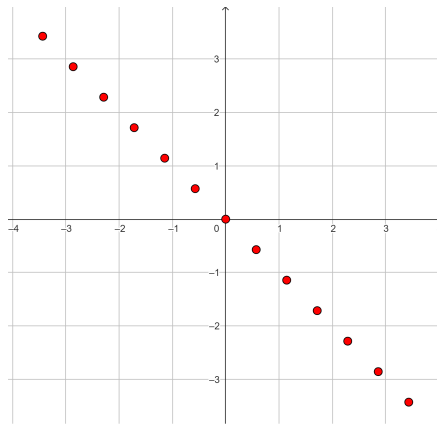


Figura 6.6: Reticulado logarítmico associado a $\mathbb{Q}(\sqrt{3})$.

Além disso, o regulador é dado por

$$|\det(\log(\sigma_1(2 + \sqrt{3})_{1 \times 1}))| = \log(2 + \sqrt{3}) \approx 0.571947$$

Exemplo 6.4.13. Generalizamos o Exemplo 6.4.12. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, com $m > 1$, um corpo quadrático real. Pelo Teorema 3.2.1, segue que $\mathcal{O}_{\mathbb{K}}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}$ e a imagem do reticulado logarítmico $\Lambda = Log(\mathcal{O}_{\mathbb{K}}^*)$ é isomorfa a $\mathbb{Z}$ em $\mathbb{R}^2$. Mais especificamente, $Log(\mathcal{O}_{\mathbb{K}}^*)$ está contido no subespaço de $\mathbb{R}^2$ que é ortogonal ao vetor unitário $(1, 1)$. De fato, se u é uma unidade fundamental de $\mathbb{K}$, então

$$\text{Log}(\pm u^e) = e(\log |\sigma_1(u)|, \log |\sigma_2(u)|),$$

para todo $e \in \mathbb{Z}$. Mas, observe que

$$\langle (\log |\sigma_1(u)|, \log |\sigma_2(u)|); (1, 1) \rangle = \log |\sigma_1(u)\sigma_2(u)| = \log |N_{\mathbb{K}}(u)| = \log 1 = 0,$$

ou seja, os vetores de $\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$, quando $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, são ortogonais a $(1, 1)$. Logo, $\Lambda = \text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ está contido no subespaço ortogonal ao vetor unitário de $\mathbb{R}^2$.

Mais geralmente, $\Lambda = \text{Log}(\mathcal{O}_{\mathbb{K}}^*)$ sempre está contido no subespaço de $\mathbb{R}^{r+s}$, que é ortogonal ao vetor unitário $(1, 1, \dots, 1)$. Além disso, é de posto completo neste subespaço. A demonstração desse fato é análoga a feita no Exemplo 6.4.13.

6.5 Raio de cobertura do reticulado logarítmico em $\mathbb{Q}(\zeta_n)$

O objetivo, desta seção, é apresentar um limite superior para o raio de cobertura do reticulado obtido via corpos ciclotômicos $\mathbb{Q}(\zeta_n)$, para qualquer $n \in \mathbb{Z}$, através do mergulho logarítmico.

A seguir, considere $\mathbb{K} = \mathbb{Q}(\zeta_n)$, $n = p_1^{e_1} \dots p_s^{e_s}$, com $n \equiv (\text{mod } 4)$, onde cada p_i é um primo distinto e $e_i \leq 1$ é inteiro ($1 \leq i \leq s$). Consideramos ainda $\Gamma = \{I \subsetneq \{1, \dots, s\}\}$. Para provarmos qual é o limitante do raio de cobertura, precisamos de alguns lemas.

Lema 6.5.1. *Para qualquer número inteiro $m \geq 1$,*

$$\sum_{k=1}^{\lfloor m/2 \rfloor} \log^2 \left(2 \cdot \text{sen} \left(\frac{\pi k}{m} \right) \right) \leq k_1 m,$$

onde k_1 é uma constante positiva independente de m .

Demonstração. Considere a seguinte função

$$f : [0, 1/2] \rightarrow \mathbb{R},$$

dada por $f(x) = \log^2(2 \text{sen}(\pi x))$. Vamos dividir o intervalo do domínio em dois: $[0, 1/6]$ e $[1/6, 1/2]$. Considere primeiramente o intervalo fechado $[1/6, 1/2] \in [0, 1/2]$. Note que a função seno é crescente neste intervalo. Logo,

$$1 = 2 \cdot \frac{1}{2} = 2 \cdot \text{sen} \left(\frac{\pi}{6} \right) \leq 2 \cdot \text{sen}(\pi x) \leq 2 \text{sen} \left(\frac{\pi}{2} \right) = 2 \cdot 1 = 2. \quad (6.5)$$

Aplicando $\log^2$ na Equação (6.5) e como $\log$ é uma função crescente, segue que

$$\log^2(1) = \log^2 \left(2 \cdot \text{sen} \left(\frac{\pi}{6} \right) \right) \leq \log^2(2 \text{sen}(\pi x)) \leq \log^2 \left(2 \text{sen} \left(\frac{\pi}{2} \right) \right) = \log^2(2) < \log 2.$$

Portanto,

$$\text{Se } x \in [1/6, 1/2], \text{ então } 0 \leq f(x) \leq \log^2(2) < \log(2). \quad (6.6)$$

Por outro lado, se $x \in [0, 1/6]$, então graficamente vemos que $2x \leq \text{sen}(\pi x)$.

Note que se $2x \leq \text{sen}(\pi x)$, então $2x \leq 4x \leq 2 \text{sen}(\pi x)$. Como $\log$ é uma função crescente, segue que $x \in [0, 1/6] \Rightarrow \log(4x) \leq \log(2 \cdot \text{sen}(\pi x)) < 0 \Rightarrow 0$. Entretanto, quando elevamos a desigualdade ao quadrado, ela muda de sentido. Assim,

$$0 < \log^2(2 \text{sen}(\pi x)) = f(x) < \log^2(4x). \quad (6.7)$$

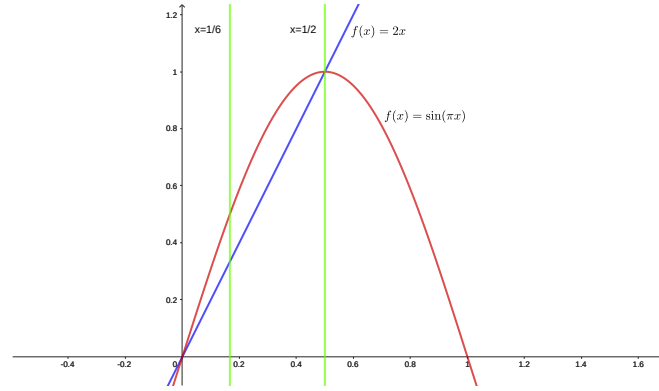


Figura 6.7: $2x \leq \sin(\pi x)$ no intervalo $[1/6, 1/2]$.

Agora, considere o somatório,

$$\sum_{k=1}^{\lfloor m/2 \rfloor} \log^2 \left(2 \sin \left(\frac{\pi k}{m} \right) \right)$$

Separamos em duas parcelas da seguinte forma:

$$\sum_{k=1}^{\lfloor m/2 \rfloor} \log^2 \left(2 \sin \left(\frac{\pi k}{m} \right) \right) = \sum_{k=1}^{\lfloor m/6 \rfloor} f \left(\frac{k}{m} \right) + \sum_{\lfloor m/6 \rfloor + 1}^{\lfloor m/2 \rfloor} f \left(\frac{k}{m} \right). \quad (6.8)$$

Da Equação (6.6), segue que a segunda parcela é limitada superiormente por $\log(2)$. Por outro lado, pela Equação (6.7), segue que a primeira parcela satisfaz

$$\sum_{k=1}^{\lfloor m/6 \rfloor} f \left(\frac{k}{m} \right) \leq \sum_{k=1}^{\lfloor m/6 \rfloor} \log^2 \left(\frac{4k}{m} \right).$$

Observe que podemos majorar a somatória por uma integral. Assim,

$$\sum_{\lfloor m/6 \rfloor + 1}^{\lfloor m/2 \rfloor} \log^2 \left(\frac{4k}{m} \right) \leq \int_0^{\lfloor m/6 \rfloor} \log^2 \left(\frac{4k}{m} \right) dk.$$

Considere $x = \frac{k}{m}$, $\frac{dx}{dk} = \frac{1}{m} \Rightarrow m dx = dk$. Assim,

$$\int_0^{\lfloor m/6 \rfloor} \log^2 \left(\frac{4x}{m} \right) dx = \int_0^{1/6} \log^2(4x) m dx = m \int_0^{1/6} \log^2(4x) dx.$$

Portanto, $\sum_{\lfloor m/6 \rfloor + 1}^{\lfloor m/2 \rfloor} \log^2(4(k/m)) \leq m \int_0^{1/6} \log^2(4x) dx$. Ainda, tome $u = 4x$ e $\frac{du}{dx} = 4 \Rightarrow \frac{du}{4} = dx$. Logo,

$$\int_0^{1/6} \log^2(4x) dx = \frac{1}{4} \int_0^{2/3} \log(u) du.$$

Agora, considere $k = \frac{1}{4} \int_0^{2/3} \log(x) dx$. A seguir, usamos a integração por partes $\int u dv = uv - \int v du$, ou seja,

$$\begin{aligned}
4k &= \int_0^{2/3} \log^2(x) dx \Rightarrow x(\log|x|)^2 - \int 2\log(x) dx = x(\log|x|)^2 - 2(x\log|x| - x) \\
&\Rightarrow x(\log|x|)^2 - 2x\log|x| + 2x \Big|_0^{2/3} = \frac{2}{3} \log^2\left(\frac{2}{3}\right) - 2 \cdot \frac{2}{3} \log\left(\frac{2}{3}\right) + 2 \cdot \frac{2}{3} \\
&\Rightarrow k = \frac{1}{4} \left[\frac{2}{3} \left(\log^2\left(\frac{2}{3}\right) - 2 \log\left(\frac{2}{3}\right) + 2 \right) \right] = \frac{1}{6} \left(\log^2\left(\frac{2}{3}\right) - 2 \log\left(\frac{2}{3}\right) + 2 \right).
\end{aligned}$$

Portanto, k é uma constante positiva independente de m . Concluimos, assim, que

$$\sum_{k=1}^{[m/6]} f\left(\frac{k}{m}\right) \leq \sum_{k=1}^{[m/6]} \log^2\left(\frac{4k}{m}\right) \leq m.k_1.$$

Agora, tome $k_1 = k + \log(2)$ (k_1 continua sendo constante positiva independente de m). Pela Equação (6.8), segue que

$$\begin{aligned}
\sum_{k=1}^{[m/2]} \log^2\left(2 \sin\left(\frac{\pi k}{m}\right)\right) &= \sum_{k=1}^{[m/6]} f\left(\frac{k}{m}\right) + \sum_{[m/6]+1}^{[m/2]} f\left(\frac{k}{m}\right) \\
&\leq m.k + \log(2) \\
&\leq mk + m \log(2) \\
&\leq m(k + \log(2)) = k_1.m,
\end{aligned}$$

o que prova o lema. $\square$

Lema 6.5.2. *Seja a um número inteiro tal que $1 \leq a \leq n/2$ e $\text{mdc}(a, n) = 1$. Se $I \in \Gamma$, então*

$$\left\| \text{Log}\left(\zeta^{\frac{-an_I}{2}} - \zeta^{\frac{an_I}{2}}\right) \right\| \leq k_2 \sqrt{n}, \quad (6.9)$$

em que k_2 é uma constante independente de n .

Demonstração. Sejam $\sigma_1, \dots, \sigma_{\varphi(n)/2}$ os monomorfismos de $\mathbb{K}$ tais que $\sigma_1 \neq \overline{\sigma_j}$, para $1 \leq i < j \leq \frac{\varphi(n)}{2}$. Pela definição de mergulho logarítmico Log em $\mathbb{K}$, segue que

$$\left\| \log\left(\zeta^{\frac{-an_I}{2}} - \zeta^{\frac{an_I}{2}}\right) \right\|^2 = \sum_{k=1}^{\varphi/2} \log^2 |\sigma_k(\zeta^{\frac{-an_I}{2}} - \zeta^{\frac{an_I}{2}})| = \sum_{k \in G} \log^2 |\zeta^{\frac{-akn_I}{2}} - \zeta^{\frac{akn_I}{2}}|, \quad (6.10)$$

onde $G = \{k \in \mathbb{Z} : 1 \leq k < n/2, \text{mdc}(k, n) = 1\} = \mathbb{Z}_n^* \setminus \{\pm 1\}$. Pela Teoria de Galois, segue que $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é o subcorpo maximal de $\mathbb{K} = \mathbb{Q}(\zeta_n)$ e $\text{Gal}(\mathbb{Q}(\zeta_n + \zeta_n^{-1})/\mathbb{Q}) \simeq \mathbb{Z}_n^* \setminus \{\pm 1\}$. Lembre que

$$\zeta_n^k = e^{\frac{2\pi k}{n}} = \cos\left(\frac{2\pi k}{n}\right) + i \sin\left(\frac{2\pi k}{n}\right).$$

Assim,

$$\begin{aligned}
\zeta^{\frac{-an_I}{2}} &= \cos\left(\frac{2\pi \frac{-akn_I}{2}}{n}\right) + i \sin\left(\frac{2\pi \frac{-akn_I}{2}}{n}\right) = \cos\left(-\frac{\pi akn_I}{n}\right) + i \sin\left(-\frac{\pi akn_I}{n}\right). \\
\zeta^{\frac{an_I}{2}} &= \cos\left(\frac{2\pi \frac{-akn_I}{2}}{n}\right) + i \sin\left(\frac{2\pi \frac{-akn_I}{2}}{n}\right) = \cos\left(\frac{\pi akn_I}{n}\right) + i \sin\left(\frac{\pi akn_I}{n}\right).
\end{aligned}$$

Logo,

$$\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}} = \cos\left(-\frac{\pi akn_I}{n}\right) + i \sin\left(-\frac{\pi akn_I}{n}\right) - \cos\left(\frac{\pi akn_I}{n}\right) - i \sin\left(\frac{\pi akn_I}{n}\right).$$

Mas, como $\sin$ é uma função ímpar e $\cos$ é função par, segue que $\sin(-x) = -\sin(x)$ e $\cos(-x) = \cos(x)$. Dessa forma,

$$\begin{aligned} \zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}} &= \cos\left(-\frac{\pi akn_I}{n}\right) + i \sin\left(-\frac{\pi akn_I}{n}\right) - \cos\left(\frac{\pi akn_I}{n}\right) - i \sin\left(\frac{\pi akn_I}{n}\right) \\ &= \cancel{\cos\left(\frac{\pi akn_I}{n}\right)} - i \sin\left(\frac{\pi akn_I}{n}\right) - \cancel{\cos\left(\frac{\pi akn_I}{n}\right)} - i \sin\left(\frac{\pi akn_I}{n}\right) \\ &= -2i \sin\left(\frac{\pi akn_I}{n}\right). \end{aligned}$$

Defina $m_I = \frac{n}{n_I}$. Dessa forma,

$$\left\| \text{Log}\left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right) \right\|^2 \stackrel{(6.9)}{=} \sum_{k \in G} \log^2 \left| 2 \left(\in \frac{\pi ak}{m_I} \right) \right| = \sum_{k \in G} \log^2 \left| 2 \left(\in \frac{\pi k}{m_I} \right) \right|.$$

Lembre que a definição de a é a mesma de k . Logo, $\{ka \mid k \in G\} = \{k \mid k \in G\}$. Agora, $m_I = \frac{n}{n_I} > 1$, e deste modo, $G \subset \{k \in \mathbb{Z} \mid 1 \leq k \leq [n/2]\}$ e

$$\left[\frac{n}{2} \right] \leq \frac{n}{2} = 2 \cdot \frac{n}{n_I} \cdot \frac{n_I}{4} \leq 2 \cdot m_I \cdot \left[\frac{n_I}{4} \right].$$

Ainda,

$$\sin\left(\frac{\pi k}{m_I}\right) = \sin\left(\frac{\pi k}{m_I} + 2\pi\right) = \sin\left(\frac{\pi(k + 2m_I)}{m_I}\right).$$

Assim,

$$\left\| \text{Log}\left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}}\right) \right\|^2 \leq \sum_{\substack{k=1 \\ (k,n)=1}}^{[n/2]} \log^2 \left| 2 \sin\left(\frac{\pi k}{m_I}\right) \right| \leq \left[\frac{n_I}{4} \right] \sum_{k=1}^{2m_I} \log^2 \left| 2 \sin\left(\frac{\pi k}{m_I}\right) \right|. \quad (6.11)$$

Agora, pelo Lema 6.5.1, segue que existe k_1 independente de m_I tais que

$$\sum_{k=1}^{m_I/2} \log^2 \left| 2 \sin\left(\frac{\pi k}{m_I}\right) \right| \leq k_1 \cdot m_I.$$

Agora, observe os seguintes fatos:

1. Observe que

$$\begin{aligned} \sum_{[m_I/2]}^{m_I+1} \log^2 \left| 2 \sin\left(\frac{\pi k}{m_I}\right) \right| &\stackrel{\substack{\sin(x)= \\ \sin(\pi-x)}}{=} \sum_{[m_I/2]}^{m_I+1} \log^2 \left| 2 \sin\left(\pi - \frac{\pi k}{m_I}\right) \right| \\ &= \sum_{[m_I/2]}^{m_I+1} \log^2 \left| 2 \sin\left(\frac{\pi(m_I - k)}{m_I}\right) \right|. \end{aligned}$$

Fazendo uma mudança de variável, segue que

$$\sum_{[m_I/2]}^{m_I+1} \log^2 \left| 2 \sin\left(\frac{\pi(m_I - k)}{m_I}\right) \right| \leq \sum_{[m_I/2]}^{k=1} \log^2 \left| 2 \sin\left(\frac{\pi(m_I - k)}{m_I}\right) \right| \leq k_1 \cdot m_I.$$

2. De modo análogo,

$$\begin{aligned} \sum_{m_I+1}^{[3m_I/2]} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi k}{m_I} \right) \right| &\stackrel{\operatorname{sen}(x) = -\operatorname{sen}(x-\pi)}{=} \sum_{m_I+1}^{[3m_I/2]} \log^2 \left| -2 \operatorname{sen} \left(\frac{\pi(k-m_I)}{m_I} \right) \right| \stackrel{|a| = |-a|}{=} \\ \sum_{m_I+1}^{[3m_I/2]} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi(k-m_I)}{m_I} \right) \right| &\leq \sum_{k=1}^{[m_I/2]} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi k}{m_I} \right) \right| \leq k_1 m_I. \end{aligned}$$

3. Ainda,

$$\begin{aligned} \sum_{[3m_I/2+1]}^{2m_I-1} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi k}{m_I} \right) \right| &\stackrel{\operatorname{sen}(x) = -\operatorname{sen}(2\pi-x)}{=} \sum_{[3m_I/2+1]}^{2m_I-1} \log^2 \left| -2 \operatorname{sen} \left(2\pi - \frac{\pi(k-m_I)}{m_I} \right) \right| = \\ \sum_{[3m_I/2+1]}^{2m_I-1} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi(2m_I-k)}{m_I} \right) \right| &\leq \sum_{k=1}^{[m_I/2]} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi k}{m_I} \right) \right| \leq k_1 m_I. \end{aligned}$$

Substituindo as informações encontradas na Equação (6.11), segue que

$$\begin{aligned} \left\| \operatorname{Log} \left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}} \right) \right\|^2 &\leq \left\lceil \frac{n_I}{4} \right\rceil \sum_{k=1}^{2m_I} \log^2 \left| 2 \operatorname{sen} \left(\frac{\pi k}{m_I} \right) \right| \\ &\leq \left\lceil \frac{n_I}{4} \right\rceil 4(k_1 m_I) = \left\lceil \frac{n_I}{4} \right\rceil \frac{n}{n_I} 4k = nk \leq 5nk. \end{aligned}$$

Se $k' = 5k$, então k' é uma constante positiva independente de n . Assim, mostramos que

$$\begin{aligned} \left\| \log \left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}} \right) \right\|^2 &\leq k'n \Rightarrow \\ \left\| \log \left(\zeta_n^{-\frac{an_I}{2}} - \zeta_n^{\frac{an_I}{2}} \right) \right\| &\leq \sqrt{k'n} = \underbrace{\sqrt{k'}}_{k_2} \sqrt{n} = k_2 \sqrt{n}, \end{aligned}$$

o que prova o lema. $\square$

Para o próximo lema, considere

$$C = \left\langle -1, \xi_a \mid 1 < a < \frac{1}{2}n, \operatorname{mdc}(a, n) = 1 \right\rangle \subset \mathcal{O}_{\mathbb{K}^+}^*, \quad (6.12)$$

onde $\mathbb{K}^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ e

$$\xi_a = \prod_{i \in I} \zeta_n^{\frac{n_I(1-a)}{2}} \left(\frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}} \right). \quad (6.13)$$

Observe que este conjunto C da Equação (6.12) foi definido no Teorema (5.4.5). Considere, também, o grupo de Galois de $\mathbb{Q}(\zeta + \zeta^{-1})$ em $\mathbb{Q}$ dado por

$$G = \{k \in \mathbb{Z} \mid 1 \leq k \leq n/2, \operatorname{mdc}(k, n) = 1\} = \mathbb{Z}_n^* \setminus \{\pm 1\}.$$

Nosso objetivo será calcular a norma euclidiana do mergulho logarítmico aplicado aos elementos geradores de C .

Lema 6.5.3. *Se $a \in G \setminus \{1\}$, então*

$$\left\| \text{Log}(\xi_a) \right\| = k_3(2^s - 1)\sqrt{n},$$

em que ξ_a é dada na Equação (6.13) e k_3 é uma constante positiva independente de n .

Demonstração. Primeiramente, note que

$$\begin{aligned} \xi_a &= \prod_{i \in I} \zeta_n^{\frac{n_I(1-a)}{2}} \left(\frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}} \right) = \prod_{i \in I} \zeta_n^{\frac{n_I}{2} - \frac{an_I}{2}} \left(\frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}} \right) \\ &= \prod_{i \in I} \frac{\zeta_n^{\frac{-an_I}{2}}}{\zeta_n^{\frac{-n_I}{2}}} \left(\frac{1 - \zeta_n^{an_I}}{1 - \zeta_n^{n_I}} \right) = \prod_{i \in I} \left(\frac{\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{an_I - \frac{an_I}{2}}}{\zeta_n^{\frac{-n_I}{2}} - \zeta_n^{n_I - \frac{n_I}{2}}} \right) \\ &= \prod_{i \in I} \left(\frac{\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}}{\zeta_n^{\frac{-n_I}{2}} - \zeta_n^{\frac{n_I}{2}}} \right). \end{aligned}$$

Assim,

$$\left\| \text{Log}(\xi(a)) \right\| = \left\| \text{Log} \left(\prod_{i \in I} \left(\frac{\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}}{\zeta_n^{\frac{-n_I}{2}} - \zeta_n^{\frac{n_I}{2}}} \right) \right) \right\|.$$

Usamos, a seguir, as propriedades básicas do logaritmo, isto é, $\log(ab) = \log(a) + \log(b)$ e $\log\left(\frac{a}{b}\right) = \log(a) - \log(b)$. Logo,

$$\begin{aligned} \left\| \sum_{I \in \Gamma} \text{Log} \left(\frac{\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}}{\zeta_n^{\frac{-n_I}{2}} - \zeta_n^{\frac{n_I}{2}}} \right) \right\| &= \left\| \sum_{I \in \Gamma} \text{Log}(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}}) - \sum_{I \in \Gamma} \text{Log}(\zeta_n^{\frac{-n_I}{2}} - \zeta_n^{\frac{n_I}{2}}) \right\| \\ &\leq \sum_{I \in \Gamma} \left\| \text{Log} \zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}} \right\| + \sum_{I \in \Gamma} \left\| \text{Log} \zeta_n^{\frac{-n_I}{2}} - \zeta_n^{\frac{n_I}{2}} \right\|. \end{aligned}$$

Pelo Lema 6.5.2, segue que

$$\left\| \text{Log} \left(\zeta_n^{\frac{-an_I}{2}} - \zeta_n^{\frac{an_I}{2}} \right) \right\| \leq k_2 \sqrt{n}.$$

Dai,

$$\begin{aligned} \left\| \text{Log}(\xi(a)) \right\| &\leq \sum_{I \in \Gamma} (k_2 \sqrt{n}) + \underbrace{\sum_{I \in \Gamma} (k_2 \sqrt{n})}_{\text{caso particular } a=1} \\ &= 2 \sum_{I \in \Gamma} (k_2 \sqrt{n}) = 2|\Gamma|(k_2 \sqrt{n}). \end{aligned}$$

Como $\Gamma = \{I \subsetneq 1, \dots, s\}$, segue que a quantidade de elementos $|\Gamma|$ é igual a $(2^s - 1)$. Assim,

$$\left\| \text{Log}(\xi(a)) \right\| \leq 2|\Gamma|(k_2 \sqrt{n}) = 2(2^s - 1)k_2 \sqrt{n} \stackrel{2k_2 = k_3}{=} k_3(2^s - 1)\sqrt{n}.$$

Onde definimos $k_3 = 2k_2$, que claramente é uma constante positiva independente de n . $\square$

Tendo provado esses três lemas, podemos finalmente demonstrar o Teorema que fornece o limitante para o raio de cobertura do reticulado logarítmico num corpo ciclotômico.

Teorema 6.5.4. *Seja $\mathbb{K} = \mathbb{Q}(\zeta_n)$ com n um inteiro que satisfaz $n \not\equiv 2 \pmod{4}$. O raio de cobertura $\mu(\text{Log}(\mathcal{O}_{\mathbb{K}}^*))$ associado ao corpo $\mathbb{K}$ satisfaz*

$$\mu(\text{Log}(\mathcal{O}_{\mathbb{K}}^*)) \leq k(2^s - 1)n,$$

em que k é uma constante positiva independente de n e s é o número de primos distintos presentes na fatoração de n .

Demonstração. Consideramos o sub-reticulado $\text{Log}(C) \subset \text{Log}(\mathcal{O}_{\mathbb{K}}^*)$, onde C igual a (6.12). Note que $\{\text{Log}(b_a) \mid a \in G \setminus \{1\}\}$ é uma base para $\text{Log}(C)$. Denote por $\lambda_i(\Lambda)$ o i -ésimo mínimo sucessivo de um reticulado Λ . Pelo Lema 6.5.3, segue que existe uma constante positiva k_3 independente de n tal que

$$\lambda_r(\text{Log}(C)) \leq \|\text{Log}(b_a)\| \leq k_3(2^s - 1)\sqrt{n},$$

para algum $a \in G \setminus \{1\}$, já que

$$\{\text{Log}(\xi_a) \mid a \in G \setminus \{1\}\}$$

tem $r = \frac{\varphi}{2} - 1$ vetores linearmente independentes e $\lambda_r(\text{Log}(C))$ é o menor ρ tal que $\text{Log}(C)$ tem r vetores linearmente independentes de norma no máximo igual a ρ . Agora, segue do Teorema 6.3.7 que

$$\mu(\text{Log}(C)) \leq \frac{\sqrt{n}}{2} \lambda_n(\text{Log}(C)),$$

e assim,

$$\mu(\text{Log}(C)) \leq \frac{\sqrt{n}}{2} k_3(2^s - 1)\sqrt{n} = \underbrace{\frac{k_3}{2}}_k n(2^s - 1) = kn(2^s - 1).$$

Ainda, $\frac{k_3}{2} > 0$, uma vez que $k_3 > 0$. Portanto, como $\text{Log}(C)$ é um sub-reticulado de $\text{Log}(\mathcal{O}_{\mathbb{K}}^*)$, segue que

$$\mu(\text{Log}(\mathcal{O}_{\mathbb{K}}^*)) \leq k(2^s - 1)n,$$

concluindo a prova do teorema. $\square$

Observação 6.5.5. A constante k é um valor real dado por

$$k = 5(\log(2) + \frac{1}{6} \left(\log^2 \left(\frac{2}{3} \right) - 2 \log \left(\frac{2}{3} \right) + 2 \right) \approx 0.3491142.$$

Exemplo 6.5.6. Considere o corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\zeta_7)$ de grau $\varphi(n) = \varphi(7) = 6$. Seu corpo maximal real $\mathbb{K}^+$ é dado por $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ e tem grau $6/2 = 3$. O grau do sub-reticulado dado por $\Lambda = \text{Log}(\mathcal{O}_{\mathbb{K}^+}^*)$ tem posto 2 em $\mathbb{R}^3$, e portanto, não é completo. Agora, vamos encontrar sua base. Para isso, considere os elementos

$$\xi_2 = \zeta_7^{-1/2} \left(\frac{1 - \zeta_7^2}{1 - \zeta_7} \right) \text{ e } \xi_3 = \zeta_7^{-1} \left(\frac{1 - \zeta_7^3}{1 - \zeta_7} \right).$$

A base de Λ é dada pelo mergulho logarítmico Log aplicado a ξ_2 e ξ_3 . Logo, a matriz geradora do reticulado é dada por

$$\mathcal{M} = \begin{bmatrix} \log |2 \cos(\pi/7)| & \log |2 \cos(3\pi/7)| & \log |2 \cos(2\pi/7)| \\ \log |1 + 2 \cos(2\pi/7)| & \log |1 + 2 \cos(6\pi/7)| & \log |1 + 2 \cos(4\pi/7)| \end{bmatrix}.$$

Assim, a matriz de Gram G é dada por

$$G = c \begin{pmatrix} 1 & -1 \\ -1 & 2 \\ \frac{-1}{2} & 1 \end{pmatrix}, \text{ com } c \approx 1.0509 \dots$$

Essa matriz de Gram é equivalente a do Exemplo (6.2.8). Portanto, $\Lambda = Log(\mathcal{O}_{\mathbb{K}^+})$ é equivalente ao reticulado hexagonal quando $\mathbb{K} = \mathbb{Q}(\zeta_7)$ e $\mathbb{K}^+ = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$.

Note que, no Exemplo 6.5.6, a partir dos conceitos de reticulado logarítmico no anel de inteiros do corpo ciclotômico $\mathbb{Q}(\zeta_7)$, obtemos o reticulado hexagonal, que já vimos anteriormente por ser a solução do problema da cobertura esférica em dimensão 2.

7 Conclusão

Vimos neste trabalho uma breve revisão de resultados de teoria algébrica dos números (Capítulo 2) e, em seguida, um estudo sobre unidades.

Para corpos quadráticos, determinamos as unidades de corpos quadráticos imaginários (Teorema 3.1.1) e para corpos quadráticos reais, um algoritmo na Seção 2.6, para encontrar a unidade fundamental do corpo (Definição 3.5.2), uma vez que através dela, pode-se encontrar as outras unidades do corpo (Teorema 3.6.2).

Para corpos cúbicos, apresentamos um limitante inferior para a unidade fundamental do corpo em termos do discriminante (Teorema 4.5.3). Além disso, neste ponto, foi apresentado o Teorema das Unidades de Dirichlet (4.2.1), que permite descrever as unidades de qualquer corpo de números a partir de raízes da unidade e de um sistema de unidades fundamentais. Apresentamos, ainda, algumas Tabela (4.2, 4.3, 4.4, 4.5) com unidades fundamentais (ou sistemas de unidades fundamentais) de alguns corpos cúbicos, que foram retiradas da referência [8] e calculadas a partir da referência [25].

Para os corpos ciclotômicos, além de uma revisão sobre raízes da unidade e os corpos ciclotômicos (Seção 5.1), apresentamos seu anel de inteiros (Teorema 5.2.16), introduzimos as unidades ciclotômicas (Definição 5.3.3) e apresentamos alguns resultados (Teoremas 5.4.5 e 5.4.7), que implicam que é suficiente trabalhar com o corpo real, uma vez que as unidades ciclotômicas são de índice finito no grupo das unidades completo.

Por fim, iniciamos o estudo de reticulados, onde apresentamos definições e principais resultados, a fim de falar do reticulado logarítmico (Definição 6.4.8), que é a maior aplicação deste trabalho. Este é definido a partir do grupo de unidades do anel de inteiros de um corpo de números, o que motivou o estudo do grupo de unidades e faz o Teorema das Unidades de Dirichlet tão importante neste contexto. Além disso, apresentamos um limitante para o raio de cobertura deste reticulado em corpos ciclotômicos (Teorema 6.5.4).

Quanto as perspectivas futuras, uma delas é a possibilidade de aprofundar o estudo do reticulado logarítmico. Em [16], algumas de suas aplicações foram apresentadas. A partir disso, há a possibilidade de analisar estas aplicações e obter novos resultados, parâmetros sobre estes reticulados e exemplos em várias dimensões. Além disso, analisar o reticulado logarítmico com outros tipos de unidades, como por exemplo as unidades circulares (Definição 5.3.8). A perspectiva é encontrar mais propriedades e exemplos que ainda não se tem na literatura, a fim de que sejam aplicados na Teoria da Informação.

Referências

- [1] EINSTEIN, A. *Como vejo o mundo*. 11. ed. Tradução de H. P. de Andrade. Rio de Janeiro: Nova Fronteira, 1981.
- [2] SHANNON, C. E. A mathematical theory of communication. *Bell System Technical Journal*, 1948.
- [3] CAMPELLO, A.; LING, C.; BELFIORE, J. Algebraic lattice codes achieve the capacity of the compound block-fading channel. *IEEE International Symposium on Information Theory (ISIT)*, p. 910–914, 2016.
- [4] CAMPELLO, A.; LING, C.; BELFIORE, J. Universal lattice codes for mimo channels. *IEEE Transactions on Information Theory*, p. 1, 2018.
- [5] CRAMER, R. et al. Recovering short generators of principal ideals in cyclotomic rings. *Proceedings of the 35th Annual International Conference on Advances in Cryptology — EUROCRYPT - Springer-Verlag New York, Inc*, v. 9666, p. 559–585, 2016.
- [6] ARAUJO, R. R. de. *Reticulados algébricos e aplicações a códigos e criptografia*. Tese (Doutorado) — UNICAMP, 2018.
- [7] ANDRADE, A. A. de. *Uma Introdução a Teoria dos Inteiros Algébricos - Volume 4*. 1. ed. São José do Rio Preto: Série Álgebra, 2021.
- [8] ALACA, S.; WILLIAMS, K. S. *Introductory Algebraic Number Theory*. 1. ed. New York: Cambridge University Press, 2004.
- [9] FACHINI, L. S. *Uma introdução aos corpos não abelianos de grau menor ou igual a 6*. Dissertação (Mestrado) — UNESP, 2021.
- [10] SAMUEL, P. *Algebraic Theory of Numbers*. Paris: HERMANN, 1970.
- [11] NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. *An Introduction to the Theory of Numbers*. 5. ed. Canada: John Wiley & Sons, 1991.
- [12] ANDRADE, A. A. de. *Uma Introdução à Teoria Elementar dos Números - Volume 6*. 1. ed. São José do Rio Preto: Série Álgebra, 2022.
- [13] ANDRADE, A. A. de. *Uma Introdução a Teoria de Grupos - Volume 1*. 1. ed. São José do Rio Preto: Série Álgebra, 2021.
- [14] RIBENBOIM, P. *Classical Theory of Algebraic Number*. 1. ed. New York: Universi-text, Springer, 2001.

-
- [15] WASHINGTON, L. *Introduction to Cyclotomic Fields*. 2. ed. New York: Springer-Verlag, 1995.
- [16] ARAUJO, R. R. de. *Anéis de inteiros de corpos de números e aplicações*. Dissertação (Mestrado) — UNESP, 2015.
- [17] BENEDITO, C. W. O. *Famílias de reticulados algébricos e reticulados ideais*. Dissertação (Mestrado) — UNESP, 2010.
- [18] IRELAND, K.; ROSEN, M. *A Classical Introduction to Modern Number Theory*. 2. ed. New York: Springer, 1990.
- [19] MICCIANCIO, D. Minkowski's theorem. *CSE 206A: Lattice Algorithms and Applications*, Disponível em: <<https://cseweb.ucsd.edu/classes/sp14/cse206A-a/lec2.pdf>>, p. 11–14, 2014.
- [20] MILES, F. C. P. *Anéis e Módulos*. São Paulo: Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo, 1972.
- [21] MATTHEWS, K. Finding the fundamental unit of a real quadratic field. *Number Theory Web*, Disponível em: <<http://www.numbertheory.org/php/unit.html>>, 2021.
- [22] ROSEN, K. *Elementary number theory and its applications*. 6. ed. [S.l.]: Pearson, 2010.
- [23] VENKOV, B. *Elementary Number theory*. University of Michigan: Wolters-Noordhoff, 1970.
- [24] KNUTH, D. *Art of computer programming - Vol. 2: Seminumerical Algorithms*. 3. ed. [S.l.]: Addison-Wesley Professional, 1997.
- [25] COHEN, H. *A Course in Computational Number Theory*. New York: Springer-Verlag, 1993.
- [26] HOFFMAN, K. M.; KUNZE, R. A. *Linear Algebra*. Prentice-Hall: Prentice-Hall Mathematics Series, 1971.
- [27] MARTINET, J. *Perfect Lattices in Euclidean Spaces*. France: Springer, 2003.
- [28] MORDELL, L. *Diophantine Equations*. London: Academic Press, 1969.
- [29] ANDRADE, A. A. de. *Uma Introdução a Teoria de Corpos - Volume 3*. 1. ed. São José do Rio Preto: Série Álgebra, 2022.
- [30] ANDRADE, A. A. de. *Uma Introdução as Estruturas Algébricas - Volume 5*. 1. ed. São José do Rio Preto: Série Álgebra, 2021.

A - Apêndice: Teorema Fundamental de Grupos Abelianos Finitamente Gerados

O teorema para classificação de grupos é dado da seguinte maneira: se G é um grupo abeliano finitamente gerado, então

1. existe um único inteiro s não negativo tal que o número de grupos cíclicos infinitos sendo somados em qualquer decomposição de G como soma (produto) direta de grupos cíclicos é precisamente s . Caso G tenha somente grupos cíclicos infinitos nessa decomposição em soma (produto) direta, ou seja, $G \simeq \mathbb{Z}^s$, o grupo G é chamado um grupo abeliano livre.
2. G é um grupo abeliano livre ou existe uma única lista de inteiros positivos (não necessariamente distintos) $m_1, m_2, \dots, m_t$, com $t \in \mathbb{N}$, tal que $m_1 > 1$, $m_1 | m_2$, $m_2 | m_3$, $\dots$, $m_{t-1} | m_t$ e

$$G \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_t} \times K,$$

onde K é um grupo abeliano livre.

3. G é um grupo abeliano livre ou existem inteiros positivos $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, com $k \in \mathbb{N}$, dos quais são únicos a menos de ordem e tais que $p_1, p_2, \dots, p_k$ são primos (não necessariamente distintos) e $\alpha_1, \alpha_2, \dots, \alpha_k$ são inteiros positivos (não necessariamente distintos) e

$$G \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}} \times K,$$

onde K é um grupo abeliano livre.

A.1 Decomposição de grupos abelianos livres finitamente gerados

Todo grupo abeliano pode ser considerado um $\mathbb{Z}$ -módulo em forma natural, uma vez que se $g \in G$ e $n \in \mathbb{Z}$, então g^n é um elemento de G . Assim, os itens da Definição 2.1.9 vale neste contexto. Como o anel $\mathbb{Z}$ dos números inteiros é um domínio principal, podemos traduzir os teoremas de estruturas, que podem ser encontrados em ([20]), para obter informações sobre os grupos abelianos finitamente gerados.

O teorema de estrutura para grupos abelianos, que neste trabalho chamamos *Teorema Fundamental de Grupos Abelianos Finitamente Gerados*, afirma que um grupo abeliano finitamente gerado é a soma direta de subgrupos cíclicos e um módulo livre.

Lembramos a seguinte definição:

Definição A.1.1. Se G é um grupo abeliano (notado aditivamente) e g um elemento de G , então a **ordem** de g é o menor inteiro positivo n tal que $n.g = 0$, e n denotado por $o(g)$. Neste caso, g é dito de **ordem finita**. Em outras palavras,

$$o(g) = \min\{n \in \mathbb{Z} \mid n > 0, \ ng = 0\}.$$

Em caso contrário, g é de **ordem infinita**. Se G é um grupo finito, a ordem de G é o número de elementos do grupo e denotamos por $o(G) = |G|$.

Considere o seguinte homomorfismo

$$\psi : \begin{cases} \mathbb{Z} & \rightarrow \frac{g\mathbb{Z}}{ag\mathbb{Z}} \\ x & \mapsto \psi(x) = gx + ag\mathbb{Z} \end{cases}$$

Assim, ψ é sobrejetor e $\ker(\psi) = a\mathbb{Z}$. Desse modo, pelo Teorema do Isomorfismo, segue que

$$\frac{\mathbb{Z}}{a\mathbb{Z}} \simeq \frac{g\mathbb{Z}}{ag\mathbb{Z}}.$$

Agora, se $g_1, g_2, \dots, g_n \in \mathbb{Z}$, então a aplicação

$$\psi : g_1\mathbb{Z} \oplus \dots \oplus g_n\mathbb{Z} \rightarrow \frac{g_1\mathbb{Z}}{ag_1\mathbb{Z}} \oplus \dots \oplus \frac{g_n\mathbb{Z}}{ag_n\mathbb{Z}},$$

definida por $\psi(a_1g_1 + \dots + a_ng_n) = (a_1g_1 + ag_1\mathbb{Z}) + \dots + (a_ng_n + ag_n\mathbb{Z})$ é um homomorfismo sobrejetor, onde $\ker(\psi) = a\mathbb{Z} \oplus \dots \oplus a\mathbb{Z}$. Portanto,

$$\frac{g_1\mathbb{Z} \oplus \dots \oplus g_n\mathbb{Z}}{a\mathbb{Z} \oplus \dots \oplus a\mathbb{Z}} \simeq \frac{g_1\mathbb{Z}}{ag_1\mathbb{Z}} \oplus \dots \oplus \frac{g_n\mathbb{Z}}{ag_n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{a\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{a\mathbb{Z}} \simeq \mathbb{Z}_a \oplus \dots \oplus \mathbb{Z}_a.$$

Proposição A.1.2. *Seja G um grupo abeliano livre finitamente gerado. Se $\{g_1, g_2, \dots, g_n\}$ e $\{h_1, h_2, \dots, h_m\}$ são duas bases de G , então $m = n$.*

Demonstração. Observe que, se $\{g_1, g_2, \dots, g_n\}$ é uma base de G e $2G = \{2g \mid g \in G\}$, então $2G \subseteq G$ é um subgrupo de G . Como cada elemento $g \in G$, pode ser descrito como $g = a_1g_1 + a_2g_2 + \dots + a_ng_n$, com $a_i \in \mathbb{Z}$, onde $i = 1, \dots, n$, podemos concluir que $2G = 2g_1\mathbb{Z} \oplus 2g_2\mathbb{Z} \oplus \dots \oplus 2g_n\mathbb{Z}$. Assim,

$$\frac{G}{2G} = \frac{g_1\mathbb{Z} \oplus g_2\mathbb{Z} \oplus \dots \oplus g_n\mathbb{Z}}{2g_1\mathbb{Z} \oplus 2g_2\mathbb{Z} \oplus \dots \oplus 2g_n\mathbb{Z}} \simeq \frac{g_1\mathbb{Z}}{2g_1\mathbb{Z}} \oplus \dots \oplus \frac{g_n\mathbb{Z}}{2g_n\mathbb{Z}} \simeq \mathbb{Z}_2 \oplus \dots \oplus \mathbb{Z}_2.$$

Dessa forma, $o(G/2G) = 2^n$. De modo análogo, se $\{h_1, h_2, \dots, h_m\}$ é uma outra base de G , então $o(G/2G) = 2^m$ e, portanto, $m = n$. $\square$

Para darmos continuidade, precisamos de alguns lemas. Mas, primeiramente precisamos das seguintes considerações.

Sejam G um grupo abeliano finitamente gerado livre de posto n e $H \neq 0$ um subgrupo de G . Considere $\mathcal{A}_{\alpha i \in \Lambda}$ o conjunto de todas as bases de G e $\mathcal{A}_\alpha = \{a_{\alpha 1}, a_{\alpha 2}, \dots, a_{\alpha n}\}$

uma base de G . Se $v \in H$, então existem inteiros únicos $\{c_{\alpha 1}, c_{\alpha 2}, \dots, c_{\alpha n}\}$ tais que $v = c_{\alpha 1}a_1 + c_{\alpha 2}a_2 + \dots + c_{\alpha n}a_n$. Seja $S = \{c_i : v \in H, i \in \Lambda, \text{ para } i = 1, 2, \dots, n\}$. Como $H \neq 0$ e $\Lambda \neq \emptyset$, segue que $S \neq \{0\}$. Note que se $v \in H$, então $-v \in H$. Assim, S possui um menor inteiro positivo c_1 e existe uma base de $\{a_1, a_2, \dots, a_n\}$ de G e $v_1 \in H$ tal que c_1 é o primeiro coeficiente. Logo,

$$v_1 = c_1a_1 + k_2a_2 + k_3a_3 + \dots + k_na_n, \text{ onde } k_2, k_3, \dots, k_n \in \mathbb{Z}.$$

Dividindo k_j por c_1 , segue que existe inteiros q_j, r_j tais que

$$k_j = c_1q_j + r_j, \text{ onde } 0 \leq r_j < c_1, \text{ para } j = 2, \dots, n.$$

Assim, $v_1 = c_1a_1 + (c_1q_2 + r_2)a_2 + \dots + (c_1q_n + r_n)a_n = c_1(a_1 + q_2a_2 + \dots + q_na_n) + r_2a_2 + \dots + r_na_n$. Deste modo,

$$v_1 = c_1u_1 + r_2a_2 + \dots + r_na_n, \text{ onde } u_1 = a_1 + q_2a_2 + \dots + q_na_n.$$

Lema A.1.3. *O conjunto $u_1, a_2, \dots, a_n$ é uma base de G ,*

Demonstração. Se $g \in G$, então existem $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ tais que

$$\begin{aligned} g &= \alpha_1a_1 + \alpha_2a_2 + \dots + \alpha_na_n \\ &= \alpha_1(u_1 - q_2a_2 - \dots - q_na_n) + \alpha_2a_2 + \dots + \alpha_na_n \\ &= \alpha_1u_1 + 1 + (\alpha_2 - q_2)a_2 + \dots + (\alpha_n - q_n)a_n, \end{aligned}$$

ou seja, $G = \langle u_1, a_2, \dots, a_n \rangle$. Agora, se $\alpha u_1 + \alpha_2a_2 + \dots + \alpha_na_n = 0$, então

$$\alpha_1(a_1 + q_2a_2 + \dots + q_na_n) + \alpha_2a_2 + \dots + \alpha_na_n = \alpha_1a_1 + (\alpha_1q_2 + \alpha_2)a_2 + \dots + (\alpha_1q_n + \alpha_n)a_n = 0.$$

Como $\{a_1, a_2, \dots, a_n\}$ é uma base de G , segue que $\alpha_i = 0$, para todo $i = 1, \dots, n$. Dessa forma, o conjunto $\{u_1, a_2, \dots, a_n\}$ é linearmente independente. Logo, $\{u_1, a_2, \dots, a_n\}$ é uma base de G . $\square$

Lema A.1.4. $r_2 = r_3 = \dots = r_n = 0$ e $v_1 = cu_1$.

Demonstração. Por hipótese, segue que $v_1 = c_1u_1 + r_2a_2 + \dots + r_na_n$, onde $u_1 = a_1 + q_2a_2 + \dots + q_na_n$, com $0 \leq r_j < c_1$ e $v_1 \in H$. Pelo Lema A.1.3, $\{u_1, a_2, \dots, a_n\}$ é uma base de G . Pela minimalidade de c_1 , segue que $r_i = 0$, onde $i = 2, \dots, n$. Portanto, $v_1 = c_1u_1$. $\square$

Lema A.1.5. *O conjunto $\{u_1, u_2, \dots, u_n\}$ é uma base de G .*

Demonstração. Pelo Lema A.1.3, segue que $\{u_1, a_2, \dots, a_n\}$ é uma base de G . Portanto,

$$G = u_1\mathbb{Z} \oplus a_2\mathbb{Z} \oplus \dots \oplus a_n\mathbb{Z}.$$

Como $A' = a_2\mathbb{Z} \oplus a_3\mathbb{Z} \oplus \dots \oplus a_n\mathbb{Z}$, segue que $G = u_1\mathbb{Z} \oplus A'$. Agora, $\{u_2, u_3, \dots, u_n\}$ é uma base de A' . Assim, $A' = u_2\mathbb{Z} \oplus u_3\mathbb{Z} \oplus \dots \oplus u_n\mathbb{Z}$. Portanto, $\{u_1, u_2, \dots, u_n\}$ é uma base de G , o que prova o lema. $\square$

Lema A.1.6. *O conjunto $\{cu_1, c_2u_2, \dots, c_mu_m\}$ é uma base de H .*

Demonstração. Pelo Lema A.1.5, segue que $\{u_1, u_2, \dots, u_n\}$ é uma base de G . Assim, o conjunto $\{c_1u_1, c_2u_2, \dots, c_mu_m\}$ é linearmente independente. Agora, $\{c_2u_2, c_3u_3, \dots, c_mu_m\} \subseteq H' \subseteq H$ e $cu_1 \in H$. Dessa forma,

$$\langle c_1u_1, c_2u_2, \dots, c_mu_m \rangle \subseteq H.$$

Por outro lado, como $\{u_1, u_2, \dots, u_n\}$ é uma base de G , segue que

$$h = \alpha_1u_1 + \alpha_2u_2 + \dots + \alpha_nu_n, \text{ onde } \alpha_i \in \mathbb{Z}, \text{ para } i = 1, 2, \dots, n.$$

Dividindo α_1 por c_1 , segue que $\alpha_1 = c_1p_1 + s_1$, onde $p_1 \in \mathbb{Z}$ e $0 \leq s_1 < c_1$. Assim, $h - c_1p_1u_1 = s_1u_1 + \alpha_2u_2 + \dots + \alpha_nu_n \in H$. Como $\{u_1, u_2, \dots, u_n\}$ é uma base de G e pela minimalidade de c , segue que $s_1 = 0$. Deste modo,

$$h - c_1p_1u_1 \in H \cap A' = H' = \langle c_2u_2, \dots, c_mu_m \rangle.$$

Como $c_1p_1u_1 \in H$, segue que $h \in \langle c_1u_1, c_2u_2, \dots, c_mu_m \rangle$. Portanto, $H = \langle c_2u_2, \dots, c_mu_m \rangle$. $\square$

Lema A.1.7. $c_1 \mid c_2$.

Demonstração. Dividindo c_2 por c_1 , segue que $c_2 = c_1q + r$, onde $q, r \in \mathbb{Z}$ e $0 \leq r < c_1$. Assim,

$$c_2u_2 - c_1u_1 = (c_1q + r)u_2 - c_1u_1 = -c_1(u_1 - qu_2) + ru_2 \in H.$$

Como $\{u_1 - qu_2, u_2, \dots, u_n\}$ é uma base de G , pela minimalidade de c_1 , segue que $r = 0$. Portanto, $c_1 \mid c_2$. $\square$

Agora, temos aparatos para provar o seguinte teorema.

Teorema A.1.8. *Sejam G um grupo abeliano livre de posto n e H um subgrupo de G .*

1. *H é um grupo abeliano livre de posto $m \leq n$.*
2. *Existem uma base $\{u_1, u_2, \dots, u_n\}$ de G e inteiros positivos $c_1, c_2, \dots, c_m \in \mathbb{N}$ tais que $c_i \mid c_{i+1}$, para todo $i = 1, 2, \dots, m-1$, de modo que $\{c_1u_1, c_2u_2, \dots, c_mu_m\}$ é uma base de H .*

Demonstração. Provamos por indução sobre a dimensão n de G . Se $H = \{0\}$, então H possui a base vazia. Se $n = 1$, então G é cíclico. Como subgrupo de grupo cíclico é cíclico, segue o resultado. Suponha que o teorema é válido para grupos abelianos livres de posto $n-1$, $n > 1$, por hipótese de indução. Fazendo uso dos Lemas A.1.3 e A.1.4, se $A' = \langle a_2, a_3, \dots, a_n \rangle$, então A' é um grupo abeliano livre de posto $n-1$. Além disso, $H' = H \cap A'$ é um subgrupo de A' . Pela hipótese de indução, segue que H' é um grupo abeliano livre de posto menor ou igual a $n-1$, digamos $m-1$, e existem uma base $\{u_2, u_3, \dots, u_n\}$ de A' e inteiros positivos $c_2, c_3, \dots, c_m$ tais que $c_i \mid c_{i+1}$ para $i = 2, 3, \dots, m-1$, e $c_2u_2, \dots, c_mu_m$ é uma base de H' . Finalmente, pelos Lemas A.1.5, A.1.6 e A.1.7 segue o resultado. $\square$

Definição A.1.9. Sejam G um grupo abeliano. O subgrupo de G , dado por $T(G) = \{g \in G \mid g \text{ tem ordem finita}\}$, é dito **subgrupo de torção**.

Definição A.1.10. Seja G um grupo abeliano. Um elemento $g \in G$ é dito **livre** se

$$\text{Anl}(g) = \{a \in \mathbb{Z}, ag = 0\}.$$

Caso contrário, g se diz elemento de **torção**.

Em outras palavras, um elemento $g \in G$ é de torção se, e somente se, existe $a \in \mathbb{Z}$, $a \neq 0$, tal que $a.g = 0$.

Definição A.1.11. Seja G um subgrupo. Se $T(G) = \langle 0 \rangle$, dizemos que G é **sem torção**; Se $T(G) \neq 0$, G é dito **com torção**; se $T(G) = G$, então G é dito **de torção**,

O objetivo é mostrar que, no contexto de grupos abelianos finitamente gerados (visto como $\mathbb{Z}$ -módulo), $G = T(M) \oplus L$, onde L é livre.

Lema A.1.12. Se G é um grupo abeliano finitamente gerado, então G é imagem homomórfica de um grupo L abeliano livre finitamente gerado.

Demonstração. Considere $g_1, g_2, \dots, g_n$ os geradores de G e $L = \underbrace{\mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}}_{n \text{ vezes}}$. Considere a $\psi : L \rightarrow G$ definida por $\psi(a_1, a_2, \dots, a_n) = a_1g_1 + a_2g_2 + \dots + a_ng_n$. Observe que ψ é um homomorfismo de grupos e também é uma aplicação sobrejetora. Portanto, $\text{Im}(\psi) = G$, o que prova o lema. $\square$

Teorema A.1.13. (Teorema fundamental dos grupos abelianos finitamente gerados) Se G é um grupo abeliano finitamente gerado com $o(G) > 1$, então

1. $G = H_1 \oplus H_2 \oplus \dots \oplus H_m \oplus K$, onde os H_i , para $i = 1, 2, \dots, m$, são subgrupos cíclicos finitos de G de ordens maiores do que 1 tal que $o(H_i) \mid o(H_{i+1})$, para $i = 1, 2, \dots, m-1$ e K é um subgrupo livre de G .
2. O subgrupo $H_1 \oplus H_2 \oplus \dots \oplus H_m$ é o subgrupo de torção de G , ou seja, $T(G) = H_1 \oplus H_2 \oplus \dots \oplus H_m$.

Demonstração. Para (1), considere um homomorfismo sobrejetor $\psi : L \rightarrow G$, com L um grupo abeliano finitamente gerado. A existência desse homomorfismo é garantida pelo Lema A.1.12. Pelo Teorema A.1.8, segue que existem uma base $\{g_1, g_2, \dots, g_n\}$ de L e inteiros positivos $a_1, a_2, \dots, a_m \in \mathbb{N}$ tais que $a_i \mid a_{i+1} + 1$, para todo $i = 1, 2, \dots, m-1$. Além disso, $\{a_1g_1, \dots, a_mg_m\}$ é uma base de $\ker(\psi)$. Dessa forma,

$$L = g_1\mathbb{Z} \oplus g_2\mathbb{Z} \oplus \dots \oplus g_n\mathbb{Z} \text{ e } \ker(\psi) = a_1g_1\mathbb{Z} \oplus a_2g_2\mathbb{Z} \oplus \dots \oplus a_mg_m\mathbb{Z}.$$

Portanto, pelo Teorema do Isomorfismo, segue que

$$G \simeq \frac{L}{\ker(\psi)} \simeq \frac{g_1\mathbb{Z}}{a_1g_1\mathbb{Z}} \oplus \dots \oplus \frac{g_m\mathbb{Z}}{a_mg_m\mathbb{Z}} \oplus g_{m+1}\mathbb{Z} \oplus \dots \oplus g_n\mathbb{Z}.$$

Assim,

$$G \simeq \frac{\mathbb{Z}}{a_1\mathbb{Z}} \oplus \dots \oplus \frac{\mathbb{Z}}{a_n\mathbb{Z}} \oplus g_{m+1}\mathbb{Z} \oplus \dots \oplus g_n\mathbb{Z},$$

isto é,

$$G \simeq \mathbb{Z}_{a_1} \oplus \dots \oplus \mathbb{Z}_{a_m} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}.$$

Note que se $a_i = 1$, então $\mathbb{Z}/a_i\mathbb{Z} = \{e\}$. Assim, sem perda de generalidade, vamos excluir todos os $a_i = 1$. Assim, existe um isomorfismo dado por

$$\bar{\psi} : \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_m} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \rightarrow G,$$

onde $a_i > 0$, $a_i \mid a_{i+1}$, para $i = 1, 2, \dots, m-1$. Tome $K = \bar{\psi}(\mathbb{Z} \oplus \cdots \oplus \mathbb{Z})$ e $H_i = \bar{\psi}(\mathbb{Z}_{a_i})$, para $i = 1, 2, \dots, m$. Assim, obtemos o que queremos e o resultado está provado. Para (2), primeiramente observe que $o(H_1 \oplus H_2 \oplus \cdots \oplus H_m) = o(H_1)o(H_2)\cdots o(H_m)$. Assim, $H = H_1 \oplus H_2 \oplus \cdots \oplus H_m$ é um subgrupo finito de G . Portanto, $H \subseteq T(G)$. Mostremos que $T(G) \subseteq H$. Seja $t \in T(G)$. Como $T(G)$ é um subgrupo de $G = H_1 \oplus H_2 \oplus \cdots \oplus H_m \oplus K$, existem $h_i \in H_i$, para $i = 1, \dots, m$ e $k \in K$, tais que $t = h_1 + h_2 + \cdots + h_m + k$. Se $o(t) = l$, então $0 = lt = lh_1 + \cdots + lh_m + lk$. Observe que $lh_1 - lh_2 + \cdots + lh_m = lk = 0$, uma vez que a soma é direta. Considere $l \neq 0$. Assim, $k = 0$. Dessa forma, $t \in H = H_1 \oplus H_2 \oplus \cdots \oplus H_m$. Portanto, $T(G) \subseteq H$. Dessa forma, concluímos que $H_1 \oplus H_2 \oplus \cdots \oplus H_m$ é o subgrupo de torção de G , o que prova o Teorema. $\square$

Observação A.1.14. Pelo Teorema A.1.13, segue que $G \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \oplus \mathbb{Z}^k$, onde $m_i \mid m_j$ para $i < j$, e $k \geq 0$ inteiro. Os inteiros $m_1, m_2, \dots, m_r$ são chamados fatores invariantes de G .

Assim, acabamos de mostrar, através Teorema A.1.13, que todo grupo abeliano finitamente gerado é uma soma direta de subgrupos cíclicos e um módulo livre. Pela Observação A.1.14, concluímos ainda que a parte livre é um produto do conjunto dos inteiros, isto é, $\coprod \mathbb{Z}$, como queríamos demonstrar neste apêndice.

Índice Remissivo

- Anel de inteiros, 23
- Anel de inteiros de corpo cúbico, 45
- Anel de inteiros de corpo quadrático, 42

- Base integral, 41
- Base potente, 41

- Característica, 28
- Corpo Ciclotômico, 144
- Corpo composto, 152
- Corpo cúbico, 30
- Corpo de números, 27
- Corpo numérico, 27
- Corpo quadrático, 30
- Corpo quártico, 30
- Corpos conjugados, 28, 32

- Densidade de centro, 172
- Densidade de empacotamento, 171
- Discriminante de um anel, 50
- Discriminante de um corpo de números, 52
- Discriminante de um polinômio, 59
- Domínio, 61

- Elemento algébrico, 26
- Elemento inteiro, 18
- Elemento primitivo, 30
- Elemento transcendente, 26
- Elementos associados, 61
- Elementos conjugados, 28
- Empacotamento esférico, 171
- Empacotamento reticulado, 171
- Equação de Pell, 67

- Fecho algébrico, 26
- Fecho inteiro, 23
- Fração contínua, 90
- Fração contínua periódica, 90
- Função Phi de Euler, 118

- Ideal fracionário, 107

- Ideal inteiro, 107
- Integralmente fechado, 25
- Inteiro algébrico, 18

- Matriz de Gram, 169
- Matriz geradora, 168
- Mínimo sucessivo, 174
- Módulo, 20
- Módulo finitamente gerado, 20
- Módulo livre, 20

- Norma, 34
- Norma de um elemento de um corpo de números, 40
- Norma mínima, 171
- Número algébrico, 18

- Ordem de grupo, 191

- Polinômio característico, 34
- Polinômio característico de um elemento de um corpo de números, 40
- Polinômio ciclotômico, 143
- Polinômio minimal, 26

- Raio de cobertura, 174
- Raiz n -ésima da unidade, 141
- Raiz n -ésima primitiva da unidade, 141
- Região fundamental, 167
- Regulador, 138
- Reticulado, 164
- Reticulado Logarítmico, 177

- Sistema de Unidades Fundamentais, 117
- Sub-reticulado, 169
- Subcorpo maximal real de $\mathbb{Q}(\zeta)$, 159
- Subgrupo das unidades ciclotômicas, 161
- Subgrupo discreto, 166

- Teorema das Unidades de Dirichlet, 115
- Teorema fundamental dos grupos abelianos finitamente gerados, 194

-
- Traço, 34
- Traço de um elemento de um corpo de números, 40
- Unidade, 61
- Unidade Ciclotômica, 156
- Unidade fundamental de corpos quadráticos, 79
- Unidade fundamental de norma -1, 78
- Unidade fundamental de norma 1, 74
- Unidades circulares, 159
- Unidades de $\mathbb{Q}(\sqrt{2})$, 65
- Unidades em corpos quadráticos imaginários, 63
- Unidades independentes, 110
- Valorização de um elemento de um corpo de números, 100
- Vetores mínimos, 174