UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de São José do Rio Preto

Unidades em Corpos Abelianos

Edcarlos Lopes Ferreira dos Santos

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Dissertação apresentada ao Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus São José do Rio Preto, como parte dos requisitos para a obtenção do título de Mestre em Matemática.

São José do Rio Preto - SP
Março - 2013

Edcarlos Lopes Ferreira dos Santos

Unidades em Corpos Abelianos

Dissertação apresentada para a obtenção do título de mestre em matemática, área de álgebra, 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 São José do Rio Preto.

BANCA EXAMINADORA
Prof. Dr. Antonio Aparecido de Andrade
Professor Doutor - IBILCE - UNESP
Orientador

Prof. Dr. Edson Donizete de Carvalho
Professor Doutor - FEIS - UNESP

Prof. Dr. Clotílzo Moreira dos Santos
Professor Doutor - IBILCE - UNESP

São José do Rio Preto, 08 de março de 2013.

A minha família,
aos meus amigos
dedico

Agradecimentos

Ao concluir este trabalho agradeço:

Primeiramente a Deus pela vida.

A minha família pelo apoio e incentivo, especialmente a minha mãe Conceição, cuja dedicação e esforço não cabem nestas poucas linhas.

A minha namorada Larissa pelo apoio nos momentos que precisei e compreensão nos momentos que faltei.

Aos meus amigos pelo companheirismo e incentivo.

Ao meu parceiro e colega de trabalho Bruno Andrade pela amizade e ajuda ao longo dessa caminhada.

Ao meu orientador, Prof. Dr. Antonio Aparecido de Andrade pela sugestão do tema e apoio prestado.

Aos membros da Banca Examinadora, pela avaliação e análise deste trabalho.

Aos docentes do IBILCE, aos docentes da FEIS-UNESP, e a todos os professores que me instruíram ao longo dessa jornada.

À CAPES pelo apoio financeiro.

A todos que de alguma forma ajudaram neste trabalho.

RESUMO

Neste trabalho, apresentamos as unidades do anel de inteiros de um corpo abeliano $\mathbb{K}$, onde damos ênfase aos corpos quadráticos e ciclôtomicos pela facilidade de descrever o anel de inteiros, bem como o grupo das unidades desses corpos. Demonstramos o Teorema das Unidades de Dirichlet que dá informações a respeito da estrutura do grupo das unidades de um corpo de números $\mathbb{K}$. Apoiados no teorema de Kronecker-Weber que diz que todo corpo abeliano $\mathbb{K}$ está contido num corpo ciclotômico $\mathbb{Q}(\xi_n)$ definimos o conceito de unidades ciclôtomicas de corpo $\mathbb{K}$, onde mostramos também que o conjunto das unidades ciclotômicas forma um grupo que tem índice finito no grupo das unidades.

Palavras-chave: anel de inteiros, unidades, corpos abelianos, unidades ciclotômicas.

ABSTRACT

In the present work, we present the units of the ring of integers of an Abelian field $\mathbb{K}$, where we emphasize quadratic and cyclotomic fields for the facility in describing the ring of integers, so as the group of units of these fields. We demonstrate the Dirichilet's Theorem of Units which give information about the group of units of a number field $\mathbb{K}$. Based on Kroenecker-Weber's theorem, which says that every abelian field $\mathbb{K}$ is contained in a cyclotomic field $\mathbb{Q}(\xi_n)$, we define the concept of cyclotomic units of the field $\mathbb{K}$, where we also show that the set of cyclotomic units form a group whose index in the group of units is finite.

Keywords: ring of integers, units, abelian field, cyclotomic unit.

Lista de símbolos

$\mathbb{N}$: Conjunto dos números naturais

$\mathbb{Z}$: Anel dos números inteiros

$\mathbb{Q}$: Corpo dos números racionais

$\mathbb{C}$: Corpo dos números complexos

$\mathbb{R}$: Corpo dos números reais

$\mathbb{K}$, $\mathbb{F}$, $\mathbb{M}$, $\mathbb{L}$: Corpos

$\mathbb{L}|\mathbb{K}$: Extensão de corpos

$\mathrm{Tr}_{\mathbb{L}|\mathbb{K}}(\alpha)$: Traço do elemento α relativo a extensão $\mathbb{L}|\mathbb{K}$

$\mathrm{N}_{\mathbb{L}|\mathbb{K}}(\alpha)$: Norma do elemento α relativa a extensão $\mathbb{L}|\mathbb{K}$

$\mathcal{O}_{\mathbb{K}}$: Anel de inteiros de $\mathbb{K}$

$\sum$: Somátorio

$\prod$: Produtório

$card(B)$: Cardinalidade do conjunto B

$\|a_{ij}\|$: Matriz $(a_{i,j})$

$a \mid b$: a divide b

A, B, R: aneis

$a \equiv b(mod\, n)$: a congruente a b módulo n

δ_{ij}: Delta de Kronecker

$[\mathbb{L} : \mathbb{K}]$: Grau da extensão $\mathbb{L} \subseteq \mathbb{K}$

$\mathbb{LK}$: Corpo composto de $\mathbb{K}$ e $\mathbb{L}$

$Gal(\mathbb{L} : \mathbb{K})$: Grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$

$o(G), \mid G \mid$: Ordem do grupo G

$\Delta[x_1, x_2, \cdots, x_k]$: Discriminante do conjunto $\{x_1, x_2, \cdots, x_k\}$

$\mathcal{O}_R(A)$: Anel de inteiros de R sobre A

ξ_n: Raiz n-ésima da unidade

$x^{(i)}$, $\sigma_i(x)$: i-ésimo conjugado de x

$a \sim b$: a associado a b

$\partial(f(x))$: Grau do polinômio $f(x)$

$\mathbb{K}^{(i)}$: i-ésimo corpo conjugado de $\mathbb{K}$

$\mathbb{Q}(\xi_n)$: n-ésimo corpo ciclotômico

$\Re(z)$: Parte real de $z \in \mathbb{C}$

U, U_n: Grupo das unidades

W: Grupo das raízes das unidades

$C,\ C_{\mathbb{K}},\ C_n$: Grupo das unidades ciclotômicas

$C_S(\mathbb{K}), C_T(\mathbb{K})$: Grupo das Unidades circulares

$h,\ h_{\mathbb{K}}$: Número de classes de ideais

χ: Caracter

f_χ: Condutor do caracter χ

φ: Função de Euller

$s_1, s_2, \cdots, s_n$: Polinômios simétricos elementares

R: Regulador de $\mathbb{K}$

$L(s, \chi)$: L série definida por χ

$\tau(\chi)$: Soma Gaussiana

$[y_h]$ ideal principal gerado por y_h.

$\mathfrak{p},\ \mathfrak{q}\ \mathfrak{m},\ \mathfrak{q}\ \ \mathfrak{J}$, etc ... : Ideais

$Cl_{\mathbb{K}}$: grupo das classes ideias

$\mathbb{Q}(\xi_n)^+$: subcorpo maximal real de $\mathbb{Q}(\xi_n)$

Sumário

Introdução

Introdução

Neste trabalho, abordamos as unidades do anel de inteiros de um corpo abeliano $\mathbb{K}$. Um elemento do anel (ou corpo) A é dito ser um inteiro sobre um de seus subanéis B se este for raiz de um polinômio mônico com coeficientes em B. Veremos que o conjunto $\mathcal{O}_A$ de todos os inteiros de A tem estrutura de um anel, e estudaremos os elementos invertíveis de $\mathcal{O}_A$ que serão chamados de unidades de $\mathbb{K}$. Veremos que o conjunto de tais unidades tem estrutura de grupo e estudaremos a estrutura de tal grupo, denominado grupo das unidades de $\mathbb{K}$. Quando nos referimos as unidades de $\mathbb{K}$ fica implícito que estamos nos referindo as unidades do anel de inteiros de $\mathbb{K}$, uma vez que em um corpo qualquer, todo elemento não nulo é invertível.

No Capitulo 1, introduzimos conceitos básicos de teoria dos números que serão úteis no decorrer deste texto, onde trabalhamos conceitos de raízes da unidade, elementos inteiros, anel de inteiros, extensão de corpos, norma e traço de uma extensão, norma de ideais e classes de números.

No Capitulo 2, mostramos alguns resultados necessários para finalmente demonstrar o Teorema das Unidades de Dirichlet, que afirma que num corpo de números $\mathbb{K}$ de grau n o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é o produto de um grupo cíclico finito, a saber o grupo das raízes da unidade contidas em $\mathbb{K}$, por um $\mathbb{Z}$-módulo livre de posto $r = r_1 + r_2 - 1$, onde r_1, r_2 são os números de imersões reais e os pares de imersões puramente complexas de $\mathbb{K}$, respectivamente.

No Capitulo 3, veremos as unidades de um corpo ciclotômico $\mathbb{Q}(\xi_n)$, onde n é uma potência de primo. Apresentamos ainda, o conceito de unidade ciclotômicas e mostramos algumas de suas propriedades, e na última seção introduzimos a definição de unidades circulares.

Neste trabalho, salvo menção contrária, os anéis considerados são comutativos e com unidades.

Capítulo 1

Resultados preliminares de teoria dos números

Neste capítulo, abordaremos alguns dos conceitos básicos de teoria algébrica dos números que serão úteis no decorrer deste trabalho. Na Seção (1.1), apresentamos algumas definições e resultados básicos de teoria dos números tais como divisibilidade, elementos associados, raízes da unidade e unidades. Na Seção (1.2), introduzimos o conceito de elementos inteiros sobre um anel e mostramos algumas propriedades importantes dos anéis de inteiros. Na Seção (1.3), trabalhamos com extensões de corpos, onde definimos o conceito de grau de um extensão e terminamos a seção com o importante Teorema do Elemento Primitivo. Na Seção (1.4), apresentamos o conceito de norma e traço de um elemento e exibimos algumas de suas propriedades elementares. Na Seção (1.5), definimos a norma de um ideal e demonstramos alguns resultados importantes. Também, definimos anéis de Dedekind e Noetheriano, e o discriminante de um corpo de números $\mathbb{K}$. Na Seção (1.6), tratamos de forma particular o anel de inteiros no caso de corpos quadráticos e de corpos ciclotômicos (no caso em que ξ é uma raiz p-ésima primitiva da unidade e p é um número primo).

1.1 Resultados básicos

Nesta seção, apresentamos conceitos básicos de teoria dos números que serão a base teórica necessária para o decorrer dos demais capítulos. As principais referências desta seção são [1] e [2].

Definição 1.1.1. *Sejam A e B anéis. Uma aplicação $\varphi : A \longrightarrow B$ é um homomorfismo, se para todo $x, y \in A$ valem:*

1. $\varphi(x + y) = \varphi(x) + \varphi(y)$.
2. $\varphi(xy) = \varphi(x)\varphi(y)$.

Um homomorfismo tal que $\varphi(x) \neq \varphi(y)$ para $x \neq y$ é dito injetor ou um monomorfismo. Um homomorfismo tal que para todo $y \in B$ existe $x \in A$ tal que $\varphi(x) = y$ é dito sobrejetor ou um epimorfismo. Um homomorfismo que é simultaneamente injetor e sobrejetor é dito ser um isomorfismo.

Definição 1.1.2. *Dois anéis A e B são ditos isomorfos quando existe um isomorfismo $\varphi : A \longrightarrow B$, e denotamos por $A \cong B$.*

Definição 1.1.3. *Sejam A um domínio, $\mathbb{K}$ seu corpo de frações e x, y elementos de $\mathbb{K}$. Dizemos que x divide y com relação a A, se existe $a \in A$ tal que $y = ax$, e denotamos por $a \mid b$.*

Definição 1.1.4. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Dizemos que $a, b \in \mathbb{K}$ são associados, quando $a \mid b$ e $b \mid a$, e denotamos por $a \sim b$.*

Definição 1.1.5. *Sejam A um domínio e $\mathbb{K}$ seu corpo de frações. Os elementos do conjunto $U = \{a \in \mathbb{K}; a \sim 1\}$, são os invertíveis de A e são chamados as unidades do anel A.*

O conjunto U da Definição 1.1.5 tem uma estrutura de grupo multiplicativo (ver [1]).

Definição 1.1.6. *Sejam $\mathbb{K}$ um corpo e $n \in \mathbb{Z}$. Um elemento $\xi \in \mathbb{K}$ é chamado uma raiz n-ésima da unidade, se ξ for raiz do polinômio $x^n - 1$, ou seja, se $\xi^n = 1$. Quando $\xi^n = 1$ e $\xi^m \neq 1$ para todo m tal que $1 \leq m \leq n-1$, dizemos que ξ é uma raiz n-ésima primitiva da unidade.*

Escrevemos $\xi = \xi_n$ para explicitar que ξ é um raiz n-ésima da unidade. Além disso, através das formulas de Moivre é possível escrever ξ_n na forma

$$\xi_n = e^{\frac{2\pi i}{n}} = \cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right).$$

Proposição 1.1.1. *Sejam $\xi_n \in \mathbb{C}$ uma raiz n-ésima primitiva da unidade e $k \in \mathbb{Z}$. Assim, ξ_n^k é uma raiz n-ésima primitiva da unidade se, e somente se, $mdc(k, n) = 1$.*

Demonstração: Seja ξ_n uma raiz n-ésima primitiva da unidade. Suponhamos que $mdc(k, n) \neq 1$, ou seja $mdc(k, n) = d$, com $d \neq 1$ e $d \neq n$. Assim, $n = dx$ para algum $x \in \mathbb{N}$, e deste modo,

$$\left(\xi_n^k\right)^d = \left(\xi_n\right)^{k\frac{n}{x}} = \left(\xi_n^n\right)^{\frac{k}{x}} = 1,$$

o que é um absurdo, uma vez que $1 < d < n$ e ξ_n é uma raiz n-ésima primitiva da unidade. Portanto, $mdc(k, n) = 1$. Reciprocamente, se $mdc(k, n) = 1$ e se $m \in \mathbb{N}$ é tal que $(\xi_n^k)^m = 1$, então $\xi_n^{km} = 1$. Assim, $n \mid km$ o que implica que $n \mid m$ uma vez que k e n são primos entre si. Portanto, ξ_n^k é uma raiz n-ésima primitiva da unidade. □

Assim, pela Proposição 1.1.1, as raízes n-ésimas primitivas da unidade são os elementos ξ^k com $mdc(k, n) = 1$, para $k = 1, 2, \cdots, n-1$. Deste modo, o número de raízes n-ésimas primitivas da unidade é dado por

$$\varphi(n) = \#\{1 \leq m \leq n-1 : mdc(m, n) = 1, m, n \in \mathbb{N}\}.$$

Proposição 1.1.2. *Sejam ξ_m uma raiz m-ésima primitiva da unidade e ξ_n uma raiz n-ésima primitiva da unidade, com $mdc(m, n) = 1$. Assim, $\xi_m^k \xi_n^l$, onde $0 \leq k \leq m-1$, $0 \leq l \leq n-1$ é uma raiz mn-ésima primitiva da unidade se, e somente se, ξ_m^k é uma raiz m-ésima primitiva da unidade e ξ_n^l é raiz n-ésima primitiva da unidade.*

Demonstração: Suponhamos que $\xi_m^k \xi_n^l$ seja uma raiz mn-ésima primitiva da unidade. Se ξ_m^k não é uma raiz m-ésima primitiva da unidade, então $mdc(m,k) = d > 1$. Assim,

$$\left(\xi_m^k \xi_n^l\right)^{\frac{mn}{d}} = \left(\left(\xi_m^k \xi_n^l\right)^{mn}\right)^{\frac{1}{d}} = 1^{\frac{1}{d}} = 1,$$

o que é um absurdo, uma vez que $\frac{mn}{d} < mn$ e $\xi_m^k \xi_n^l$ é uma raiz mn-ésima primitiva da unidade. Reciprocamente, se ξ_m^k é uma raiz m-ésima primitiva da unidade e ξ_n^l é uma raiz m-ésima primitiva da unidade, então $mdc(k,m) = mdc(l,n) = 1$. Assim,

$$\left(\xi_m^k \xi_n^l\right)^a = 1 \Leftrightarrow \xi_m^{ka} = \xi_n^{-la} \Leftrightarrow \xi_m^{kan} \xi_n^{-lan} = 1 \Leftrightarrow \left(\xi^k\right)^{na} = 1 \Leftrightarrow m \mid na.$$

Como $mdc(m,n) = 1$, segue que $m \mid a$. Analogamente, mostra-se que $n \mid a$. Portanto, $mn \mid a$ e assim

$$\left(\xi_m^k \xi_n^l\right)^{mn} = \left(\xi_m^m\right)^{kn} \left(\xi_n^n\right)^{lm} = 1.$$

Deste modo, mn é a menor potência para a qual se tem $\left(\xi_m^k \xi_n^l\right)^{mn} = 1$, e portanto, $\xi_m^k \xi_n^l$ é uma raiz mn-ésima primitiva da unidade. □

1.2 Elementos inteiros

O objetivo desta seção é introduzir o conceito de elementos inteiros sobre um anel, e exibir alguns resultados importantes, muitos dos quais teremos o cuidado de demonstra-los, as principais referências desta seção são [1], [2] e [3].

Definição 1.2.1. *Sejam $A \subseteq R$ anéis. Um elemento $\alpha \in R$ é dito ser inteiro sobre A se α é raiz de um polinômio mônico com coeficientes em A, ou seja, se existem $a_0, a_1, \cdots, a_{n-1} \in A$, não todos nulos, tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, com $a_i \in A$ e $0 \leq i \leq n$. Quando todo elemento $b \in R$ é um inteiro sobre A dizemos que R é inteiro sobre A.*

Sejam $A = \mathbb{Z}$ e $\mathbb{Q} \subseteq \mathbb{K}$ uma extensão de corpos. Se $\alpha \in \mathbb{K}$ for inteiro sobre A dizemos que α é um *inteiro algébrico*.

Proposição 1.2.1. *Sejam R um anel, A um subanel de R e α um elemento de R. As seguintes afirmações são equivalentes:*

1. *α é inteiro sobre A.*
2. *O anel $A[\alpha] = \left\{ \sum_i a_i \alpha^i ; a_i \in A \right\}$ é um A-módulo finitamente gerado.*
3. *Existe um subanel B de R que contém A e α que é um A-módulo finitamente gerado.*

Demonstração: Para 1) $\Rightarrow$ 2), seja M um A-submódulo de R gerado por $\{1, \alpha, \cdots, \alpha^{n-1}\}$. Como α é inteiro sobre A, segue que

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

com a_i não todo nulos. Assim,

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0,$$

e portanto, $\alpha^n \in M$. Mostramos agora, que $M = A[\alpha]$. Para isso, devemos mostrar que $\alpha^j \in M$, para todo $j \in \mathbb{N}$. Para $j \leq n$, tem-se claramente que $\alpha^j \in M$. Agora, suponhamos que $\alpha^j \in M$ e mostramos que $\alpha^{j+1} \in M$. Como $\alpha^j \in M$, segue que $\alpha^j = \sum_{i=0}^{n-1} s_i \alpha^i$, onde $s_i \in A$. Assim,

$$\begin{aligned}
\alpha^{j+1} &= \alpha^j \alpha = \left(\sum_{i=0}^{n-1} s_i \alpha^i \right) \alpha \\
&= (s_{n-1}\alpha^{n-1} + \cdots + s_0)\alpha \\
&= s_{n-1}\alpha^n + s_{n-2}\alpha^{n-1} + \cdots + s_0\alpha \\
&= s_{n-1}(a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) + s_{n-2}\alpha^{n-1} + \cdots + s_0\alpha \\
&= (s_{n-2} - a_{n-1}s_{n-1})\alpha^{n-1} + (s_{n-3} - a_{n-2}s_{n-1})\alpha^{n-2} + \cdots + (s_0 - a_1 s_{n-1})\alpha - a_0 s_{n-1}.
\end{aligned}$$

Como cada termo entre parênteses é um elemento de A, segue que $\alpha^{j+1} \in M$, para todo $j \in \mathbb{N}$. Assim, $A[\alpha] \subseteq M$. Como $M \subseteq A[\alpha]$, uma vez que M é gerado por $\{1, \alpha, \cdots, \alpha^{n-1}\}$, segue que $A[\alpha] = M$. Portanto, $A[\alpha]$ é um A-módulo finitamente gerado.

Para 2) $\Rightarrow$ 3), considerando $B = A[\alpha]$, segue que B é finitamente gerado, $A \subseteq B$ e $\alpha \in B$. Finalmente, para 3) $\Rightarrow$ 1), por hipótese, $B = A[\alpha]$ é um A-módulo finitamente gerado. Se $\{y_1, y_2, \cdots, y_n\} \subseteq B$ é um conjunto de geradores de B, então

$$B = \sum_{i=1}^{n} a_i y_i,$$

onde $a_i \in A$ para $i = 1, 2, \cdots, n$. Assim, $\alpha y_i \in B$, para todo $1 \leq i \leq n$, uma vez que $\alpha \in B$. Assim,

$$\alpha y_i = \sum_{j=1}^{n} a_{ij} y_j$$

e portanto,

$$\alpha y_i - \sum_{j=1}^{n} a_{ij} y_j = 0.$$

Deste modo,

$$\sum_{j=1}^{n} (\delta_{ij}\alpha - a_{ij}) y_j = 0,$$

onde $\delta_{ij} = \begin{cases} 1 & \text{se} \quad i = j \\ 0 & \text{se} \quad i \neq j. \end{cases}$ Seja $d = \det(\delta_{ij}\alpha - a_{ij}) = \alpha^n + \cdots + a_0$, pela *Regra de Cramer*, segue que $dy_i = 0$, para todo $i = 1, 2, \cdots, n$. Assim, $dy = 0$ para todo $y \in B$. Em particular, $d1 = d = 0$. Deste modo, $d = \alpha^n + \cdots + a_0 = 0$, e assim o elemento α é inteiro sobre A. □

Proposição 1.2.2. *Seja R um anel, A um subanel de R e $\{r_1, r_2, \cdots, r_n\}$ um conjunto finito de elementos de R. Se r_i é inteiro sobre $A[r_1, r_2, \cdots, r_{i-1}]$, para todo $i = 1, 2, \cdots, n$, então $A[r_1, r_2, \cdots, r_n]$ é um A-módulo finitamente gerado.*

Demonstração: A prova é feita por indução sobre n. Para $n = 1$ o resultado segue da Proposição 1.2.1. Para $n \geq 2$ assumimos que $B = A[r_1, r_2, \cdots, r_{n-1}]$ é um A-módulo finitamente gerado, e sejam $\{y_1, y_2, \cdots, y_p\}$ um conjunto gerador de B sobre A, isto é,

$$B = \sum_{i=1}^{p} A y_i.$$

Como r_n é inteiro sobre B, pela Proposição 1.2.1, segue que $B[r_n]$ é um B-módulo finitamente gerado. Assim, existe $\{s_1, s_2, \cdots, s_q\} \subseteq B[r_n]$ tal que

$$B[r_n] = \sum_{j=1}^{q} Bs_j = \sum_{j=1}^{q} \left(\sum_{i=1}^{p} Ay_i \right) s_j = \sum_{i,j} Ay_i s_j.$$

Portanto, $B[r_n] = A[r_1, r_2, \cdots, r_n]$ é um A-módulo finitamente gerado por $\{y_i s_j\}$, onde $1 \leq i \leq p$ e $1 \leq j \leq q$. □

Proposição 1.2.3. *Sejam $A \subseteq B \subseteq R$ anéis. Assim, R é inteiro sobre A se, e somente se, R é inteiro sobre B e B é inteiro sobre A.*

Demonstração: Se R é inteiro sobre A, então para $\alpha \in R$, existem $a_0, a_1, \cdots, a_{n-1} \in A$, tal que

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

Como $A \subseteq B$, segue que $a_0, a_1, \cdots, a_{n-1} \in B$, e assim α é um inteiro sobre B, e portanto R é inteiro sobre B. Agora, seja $\beta \in B$. Como $B \subseteq R$, segue que $\beta \in R$ e como por hipótese R é inteiro sobre A, segue que β é inteiro sobre A. Portanto, B é inteiro sobre A. Reciprocamente, se R é inteiro sobre B e B é inteiro sobre A, para $\alpha \in R$, então existem $b_0, b_1, \cdots, b_{n-1} \in B$, não todos nulos, tal que

$$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0.$$

Assim, α é inteiro sobre $A[b_0, b_1, \cdots, b_{n-1}]$ e como B é inteiro sobre A, segue da Proposição 1.2.2 que $A[b_0, b_1, \cdots, b_{n-1}, \alpha]$ é um A-módulo finitamente gerado. Assim, pela Proposição 1.2.1, segue que α é um inteiro sobre A e assim R é inteiro sobre A. □

Definição 1.2.2. *Sejam $A \subseteq R$ anéis.*

1. *O conjunto de todos os elementos de R que são inteiros sobre A é um subanel de R chamado de anel de inteiros de R sobre A, ou ainda, o fecho inteiro de R sobre A, e será denotado por $\mathcal{O}_R$.*

2. *Se A é um domínio de integridade e $\mathbb{K}$ é o seu corpo de frações, o fecho inteiro de A em $\mathbb{K}$ é chamado de fecho inteiro de A, e denotado por $\mathcal{O}_{\mathbb{K}}$.*

Definição 1.2.3. *Um domínio de integridade A é dito integralmente fechado se for o seu próprio fecho inteiro.*

Definição 1.2.4. *Sejam R um anel e $\mathbb{K}$ um corpo contido em R. Um elemento $\alpha \in R$ é chamado algébrico sobre $\mathbb{K}$ se existem elementos $a_0, a_1, \cdots, a_n \in \mathbb{K}$, não todos nulos, tal que*

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0 \tag{1.1}$$

Se α não é algébrico sobre $\mathbb{K}$ dizemos que α é transcendente.

Sendo $\mathbb{K}$ um corpo e assumindo que $a_n \neq 0$ podemos multiplicar a Equação (1.1) por $a_n^{-1} \in \mathbb{K}$, e assim notamos que α é inteiro sobre $\mathbb{K}$. Logo, se α é inteiro sobre $\mathbb{K}$, então α é algébrico sobre $\mathbb{K}$.

1.3 Extensão de corpos

Nesta seção, apresentamos alguns resultados de extensão de corpos que serão úteís no decorrer desse trabalho. O principal resultado desta seção é o Teorema 1.3.2, conhecido como Teorema do Elemento Primitivo. A principal referência desta seção é [1].

Definição 1.3.1. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos.*

1. *Dizemos que $\mathbb{L}$ é uma extensão de $\mathbb{K}$, ou simplesmente, que $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão de corpos.*

2. *O corpo $\mathbb{L}$ pode ser visto como um $\mathbb{K}$-espaço vetorial, e assim definimos o grau da extensão como sendo a dimensão de $\mathbb{L}$ como um $\mathbb{K}$ espaço vetorial, ou seja,*

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

No caso em que $[\mathbb{L} : \mathbb{K}]$ é finita, dizemos que a extensão é finita.

3. Quando todo elemento de $\mathbb{L}$ for algébrico sobre $\mathbb{K}$ dizemos que a extensão é algébrica.

Proposição 1.3.1. *Sejam $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$ extensões de corpos. Se $\mathbb{K} \subseteq \mathbb{L}$ e $\mathbb{L} \subseteq \mathbb{M}$ são extensões algébricas, então $\mathbb{K} \subseteq \mathbb{M}$ é uma extensão algébrica e vale*

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

Demonstração: Pela Proposição 1.2.3, segue que $\mathbb{K} \subseteq \mathbb{M}$ é algébrica. Agora, se $\{x_i\}_{i\in I}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $\{y_j\}_{j\in J}$ é uma base de $\mathbb{M}$ sobre $\mathbb{L}$, então $\{x_i y_j\}_{(i,j)\in I\times J}$ é um conjunto gerador de $\mathbb{M}$ sobre $\mathbb{K}$. Finalmente, se $\sum_{i,j} a_{ij}x_i y_j = 0$, com $a_{ij} \in \mathbb{K}$, então $\sum_{j\in J}\left(\sum_{i\in I} a_{ij}x_i\right) y_j = 0$ mas, como $\{y_j\}_{j\in J}$, é uma base e portanto linearmente independente, devemos ter, $\left(\sum_{i\in I} a_{ij}x_i\right) = 0$ para todo $j \in J$ mas, como $\{x_i\}_{i\in I}$ é uma base, segue que $a_{ij} = 0$ para todo $(i,j) \in I \times J$. Portanto, $\{x_i y_j\}_{(i,j)\in I\times J}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$, e assim, $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$. □

Definição 1.3.2. *Uma extensão de corpos $\mathbb{K} \subseteq \mathbb{L}$ é dita ser uma extensão simples se existir $\alpha \in \mathbb{L}$ tal que $\mathbb{K}(\alpha) = \mathbb{L}$.*

Definição 1.3.3. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ corpos e $\alpha \in \mathbb{L}$. O polinômio mônico com coeficientes em $\mathbb{K}$ de menor grau tal que α é raiz é chamado de polinômio minimal de α.*

Proposição 1.3.2. *Seja $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos. Se $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$, então o polinômio minimal de α é irredutível e único.*

Demonstração: Seja $p(x) \in \mathbb{K}[x]$ o polinômio minimal de α de grau n. Se $p(x)$ for redutível em $\mathbb{K}[x]$, então existem polinômios $f(x), g(x) \in \mathbb{K}[x]$ tal que $p(x) = f(x)g(x)$ com $1 \leq \partial(f(x)), \partial(g(x)) \leq n-1$, assim $p(\alpha) = f(\alpha)g(\alpha) = 0 \Rightarrow f(\alpha) = 0$ ou $g(\alpha) = 0$. Em qualquer um dos casos segue que α é raiz de um polinômio em $\mathbb{K}[x]$ com grau menor que n, o que é uma contradição. Suponhamos, agora, que o polinômio minimal $p(x)$ de α não seja único. Deste modo, se $p(x), q(x) \in \mathbb{K}[x]$ são dois polinômios minimais de α, distintos e de grau n então $g(x) = p(x) - q(x) \in \mathbb{K}[x]$ e tem grau menor que n, uma vez

que $p(x)$ e $q(x)$ são mônicos de grau n, e além disso α é raiz de $g(x)$ o que contradiz a hipótese. $\square$

Teorema 1.3.1. *Se $\mathbb{K}$ é um corpo de característica zero, $\mathbb{L}$ é uma estensão de $\mathbb{K}$ de grau n, e $\mathbb{M}$ é um corpo algébricamente fechado, então existem n $\mathbb{K}$-monomorfismos distintos de $\mathbb{L}$ em $\mathbb{M}$.*

Demonstração: A afirmação é verdadeira se $\mathbb{L} = \mathbb{K}(\alpha)$ é uma extensão simples de $\mathbb{K}$, uma vez que o polinômio minimal de α sobre $\mathbb{K}$ tem n raízes distintas $\alpha_1, \alpha_2, \cdots, \alpha_n$ em $\mathbb{M}$. Logo, existem n $\mathbb{K}$-monomorfismos $\sigma_i : \mathbb{L} \longrightarrow \mathbb{M}$, tal que $\sigma_i(\alpha) = \alpha_i$, para $i = 1, 2, \cdots, n$. No caso em que $\mathbb{L}$ não é uma extensão simples de $\mathbb{K}$, a demonstração é feita por indução sobre n. Seja $\alpha \in \mathbb{L}$ e a extensão de corpos $\mathbb{K} \subseteq \mathbb{K}(\alpha) \subseteq \mathbb{L}$, onde $q = [\mathbb{K}(\alpha) : \mathbb{K}]$. Podemos assumir que $q > 1$ e assim existem q $\mathbb{K}$-monomorfismos distintos de $\mathbb{K}(\alpha)$ em $\mathbb{M}$. Como α e $\sigma_i(\alpha)$ tem o mesmo polinômio minimal, para todo $i = 1, 2, \cdots, q$, segue que os corpos $\mathbb{K}(\alpha)$ e $\mathbb{K}(\sigma_i(\alpha))$ são isomorfos. Seja $\mathbb{L}_i$ uma extensão de $\mathbb{K}(\sigma_i(\alpha))$ que é isomorfa a $\mathbb{L}$, com θ_i sendo tal isomorfismo. Assim, $\mathbb{K}(\sigma_i(\alpha))$ é de característica zero e

$$[\mathbb{L}_i : \mathbb{K}(\sigma_i(\alpha))] = [\mathbb{L} : \mathbb{K}(\sigma_i(\alpha))] = \frac{n}{q} < n.$$

Logo, pela hipótese de indução, segue que existem $\frac{n}{q}$ $\mathbb{K}(\sigma_i(\alpha))$-monomorfismo distintos τ_{ij} de $\mathbb{L}_i$ em $\mathbb{M}$ para $1 \leq j \leq \frac{n}{q}$. Portanto, a composição $\tau_{ij} \circ \theta_i : \mathbb{L} \longrightarrow \mathbb{M}$ é um $\mathbb{K}$-monomorfismo e como existem $q\frac{n}{q} = n$ aplicações $\tau_{ij} \circ \theta_i$, segue que existem n $\mathbb{K}$-monomorfismo de $\mathbb{L}$ em $\mathbb{M}$. Além disso, são todos distintos, uma vez que se $i \neq i'$, então $\tau_{ij} \circ \theta_i$ e $\tau_{i'j} \circ \theta_{i'}$ diferem em $\mathbb{K}(\alpha)$. Além disso, quando $i = i'$ mas $j \neq j'$, segue que $\tau_{ij} \circ \theta_i$ e $\tau_{ij'} \circ \theta_i$ diferem em $\mathbb{L}_i$. $\square$

Teorema 1.3.2 (Teorema do elemento primitivo)**.** *Se $\mathbb{K}$ é um corpo de característica zero e $\mathbb{L}$ é uma extensão de grau n sobre $\mathbb{K}$, então existem $\alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$, onde α é dito um elemento primitivo.*

Demonstração: Suponhamos que $\mathbb{K}$ é de característica zero e portanto de cardinalidade infinita. Pelo Teorema 1.3.1, existem n $\mathbb{K}$-monomorfismo distintos σ_i de $\mathbb{L}$ num corpo

algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$. Para cada $i \neq j$ tem-se que o conjunto $V_{ij} = \{\beta \in \mathbb{L};\ \sigma_i(\beta) = \sigma_j(\beta), i \neq j\}$ é um $\mathbb{K}$-subespaço vetorial de $\mathbb{L}$, uma vez que se $\alpha, \beta \in V_{ij}$, então para $i \neq j$ segue que $\sigma_i(\alpha\beta^{-1}) = \sigma_i(\alpha)\sigma_i(\beta)^{-1} = \sigma_j(\alpha)\sigma_j(\beta)^{-1} = \sigma_j(\alpha\beta^{-1})$. Além disso, $V_{ij} \subsetneq \mathbb{L}$ uma vez que existem elementos $\gamma \in \mathbb{L}$ tal que $\sigma_i(\gamma) \neq \sigma_j(\gamma)$. Como $\mathbb{K}$ é infinito, segue da algebra linear que $\bigcup_{i,j} V_{ij} \subsetneq \mathbb{L}$. Agora, se $\alpha \in \mathbb{L} - \bigcup_{i,j} V_{ij}$, então os σ_i's são dois a dois distintos, e assim o polinômio minimal de α têm no mínimo n raízes distintas em $\mathbb{F}$. Assim, $[\mathbb{K}(\alpha) : \mathbb{K}] \geq n$ e como $\mathbb{K}(\alpha) \subseteq \mathbb{L}$ e $[\mathbb{L} : \mathbb{K}] = n$, segue que $\mathbb{L} = \mathbb{K}(\alpha)$. $\square$

Definição 1.3.4. *Dizemos que um corpo $\mathbb{K}$ é um corpo de números se for uma extensão finita do corpo dos números racionais $\mathbb{Q}$, isto é, $\mathbb{K} = \mathbb{Q}(\theta)$, tal que $[\mathbb{Q}(\theta) : \mathbb{Q}] < \infty$. Quando o grau da extensão $\mathbb{Q}(\theta) \mid \mathbb{Q}$ for igual a 2, dizemos que $\mathbb{K} = \mathbb{Q}(\theta)$ é um corpo quadrático.*

Definição 1.3.5. *Um corpo ciclotômico, é um corpo gerado por uma raiz n-ésima da unidade sobre o corpo $\mathbb{Q}$ dos números racionais, e denotado por $\mathbb{Q}(\xi_n)$*

Definição 1.3.6. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos e $Aut(\mathbb{L})$ o grupo dos automorfismo de $\mathbb{L}$. Definimos o grupo de Galois de $\mathbb{L}$ sobre $\mathbb{K}$ como sendo*

$$Gal(\mathbb{L} : \mathbb{K}) = \{\sigma \in Aut(\mathbb{L}); \sigma(x) = x,\ \textit{para todo } x \in \mathbb{K}\}.$$

A extensão $\mathbb{K} \subseteq \mathbb{L}$ é dita ser Galoisiana ou de Galois, se a ordem do grupo de Galois for igual ao grau da extensão, isto é, se $o(Gal(\mathbb{L} : \mathbb{K})) = [\mathbb{L} : \mathbb{K}]$. Se $Gal(\mathbb{L} : \mathbb{K})$ é abeliano (respectivamente, cíclico) dizemos que a extensão $\mathbb{K} \subseteq \mathbb{L}$ é abeliana (respectivamente, ciclíca).

1.4 Traço e norma

Nesta seção, apresentamos os conceitos de traço e norma de um elemento relativo a uma extensão, e exibimos algumas de suas propriedades, onde algumas das quais por conveniência não serão demonstradas. A bibliografa usada nesta seção é [4].

Definição 1.4.1. *Seja $\mathbb{K} \subseteq \mathbb{L}$ uma extensão de corpos de grau n e sejam $\sigma_1, \sigma_2, \cdots, \sigma_n$ os $\mathbb{K}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. Dado um elemento $\alpha \in \mathbb{L}$, o traço e a norma de α com respeito a extensão $\mathbb{K} \subseteq \mathbb{L}$ são definidos como sendo*

$$Tr_{\mathbb{L}|\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad e \quad N_{\mathbb{L}|\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

respectivamente.

Dentre as principais propriedades para o traço e a norma, destacamos as seguintes.

Propriedade 1.4.1. *Sejam $\mathbb{M} \subseteq \mathbb{K} \subseteq \mathbb{L}$ extensões de corpos tal que $[\mathbb{L} : \mathbb{K}] = n$. Se $\alpha, \beta \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:*

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

Quando não houver risco de ambiguidade sobre a extensão $\mathbb{K} \subseteq \mathbb{L}$ que estamos considerando, denotamos o traço e a norma de $\alpha \in \mathbb{L}$, simplesmente por $\mathrm{Tr}(\alpha)$ e $\mathrm{N}(\alpha)$, respectivamente.

1.5 Anel de inteiros algébricos

Nesta seção, explicitamos o anel dos inteiros algébricos de alguns corpos de números, onde calculamos explicitamente o anel dos inteiros algébricos de um corpo quadrático $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados, e para os corpos $\mathbb{Q}(\xi)$, onde aqui ξ denota uma raiz p-ésima primitiva da unidade com p um número primo. O caso geral, por sua

complexidade, não será tratado nesse trabalho, e as principais referências dessa seção são [1] e [2]. Começamos com o anel de inteiros algébricos nos corpos quadráticos.

Teorema 1.5.1. *Se d é um inteiro racional livre de quadrados, então o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ é dado por*

1. $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\sqrt{d}\right]$ *se* $d \equiv 2(mod\,4)$ *ou* $d \equiv 3(mod\,4)$.
2. $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1}{2} + \frac{\sqrt{d}}{2}\right]$ *se* $d \equiv 1(mod\,4)$.

Demonstração: Um elemento $\alpha \in \mathbb{Q}(\sqrt{d})$ tem a forma $\alpha = r + s\sqrt{d}$, onde $r, s \in \mathbb{Q}(\sqrt{d})$. Podemos, portanto escrever $\alpha = \frac{a+b\sqrt{d}}{c}$, onde $a, b, c \in \mathbb{Z}$ são primos entre si e $c > 0$. Agora, α é um inteiro sobre $\mathbb{Z}$ se, e somente se, for raiz de um polinômio mônico $P(t)$ com coeficientes em $\mathbb{Z}$. Assim, o conjugado $\alpha^{(1)} = \frac{a-b\sqrt{d}}{c}$, é também raiz de $P(t)$, e portanto, podemos fatorar $P(t)$ na forma

$$P(t) = \left(t - \left(\frac{a + b\sqrt{d}}{c}\right)\right)\left(t - \left(\frac{a - b\sqrt{d}}{c}\right)\right).$$

Assim, os coeficientes de $P(t)$, devem ser elementos de $\mathbb{Z}$, isto é,

$$\frac{a^2 - b^2 d}{c^2} \in \mathbb{Z} \tag{1.2}$$

e

$$\frac{2a}{c} \in \mathbb{Z}. \tag{1.3}$$

Como a e c são primos entre si, segue da Equação (1.3) que $c = 1$ ou $c = 2$. Se $c = 1$, então obviamente α é um inteiro algébrico, e assim $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$. Se $c = 2$, então devemos ter a, b de mesma paridade e $\frac{a^2-b^2d}{4} \in \mathbb{Z}$. Portanto, $a^2 - b^2 d \equiv 0(mod\,4)$. Agora, um número ímpar da forma $2k + 1$ ao quadrado satisfaz $4k^2 + 4k + 1 \equiv 1(mod\,4)$. Portanto, $a^2 \equiv 1 \equiv b^2(mod\,4)$ e assim $d \equiv 1(mod\,4)$. Reciprocamente, se $d \equiv 1(mod\,4)$, então para a, b ímpares (o caso par é trivial) tem-se que α é um inteiro sobre $\mathbb{Z}$ uma vez que valem as Equações (1.2) e (1.3). Se $a = 2k + 1$, $b = 2q + 1$, com $k, q \in \mathbb{Z}$, como $d \equiv 1(mod\,4)$ segue que $d = 4w + 1$ para algum inteiro w. Assim

$$a^2 - b^2 d = 4k^2 + 4k - 16q^2 w - 16q - 4w - 4q^2 - 4q \equiv 0(mod\ 4).$$

Logo, valem as Equações (1.2) e (1.3), e assim $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1}{2} + \frac{\sqrt{d}}{2}\right]$. □

Agora, similarmente ao Teorema 1.5.1, analisamos o anel dos inteiros algébricos de um corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\xi)$, onde ξ é uma raiz p-ésima primitiva da unidade com p um número primo ímpar.

Teorema 1.5.2. *Se $\mathbb{K} = \mathbb{Q}(\xi)$, onde ξ é uma raiz p-ésima primitiva da unidade, com p um número primo ímpar, então $\mathcal{O}_{\mathbb{K}}$ é um grupo abeliano livre com base $\{1, \xi, \xi^2, \cdots, \xi^{p-2}\}$, ou seja, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi]$.*

Demonstração: Tem-se que $\{1, \xi, \xi^2, \cdots, \xi^{p-2}\}$ é linearmente independente sobre $\mathbb{Q}$, pois caso contrário, ξ seria uma raiz de um polinômio com grau menor do que $p-2$, contrariando a hipótese. Assim, se $x \in \mathcal{O}_{\mathbb{K}}$, então existem números racionais $a_0, a_1, \cdots, a_{p-2}$, tal que

$$x = a_0 + a_1\xi + \cdots + a_{p-2}\xi^{p-2}. \tag{1.4}$$

Agora, provamos que cada a_i pertence a $\mathbb{Z}$, para $i = 1, 2, \cdots, p-2$. Multiplicando a Equação (1.4) por ξ tem-se que

$$x\xi = a_0\xi + a_1\xi^2 + \cdots + a_{p-2}\xi^{p-1}. \tag{1.5}$$

Subtraindo a Equaçao (1.5) de (1.4) tem-se que

$$x(1-\xi) = a_0(1-\xi) + a_1(\xi - \xi^2) + \cdots + a_{p-2}(\xi^{p-2} - \xi^{p-1}). \tag{1.6}$$

Tem-se que os traços de $\xi, \xi^2, \cdots, \xi^{p-2}$ em $\mathbb{Q}(\xi)|\mathbb{Q}$ são todos iguais uma vez que os elementos são conjugados, e portanto

$$\mathrm{Tr}(x(1-\xi)) = \mathrm{Tr}(a_0(1-\xi)) = a_0\mathrm{Tr}(1-\xi) = a_0[(p-1)+1] = a_o p.$$

Para mostrar que $a_0 \in \mathbb{Z}$, calculamos $\mathrm{Tr}(x(1-\xi))$. Para isso, sejam $x_1, x_2, \cdots, x_{p-1} \in \mathcal{O}_{\mathbb{K}}$ os conjugados de x. Assim,

$$\mathrm{Tr}(x(1-\xi)) = x_1(1-\xi) + x_2(1-\xi^2) + \cdots + x_{p-1}(1-\xi^{p-1}) = (1-\xi)x' \in \mathcal{O}_{\mathbb{K}}(1-\xi)$$

uma vez que $\frac{1-\xi^{p+1}}{1-\xi} = 1 + \xi + \cdots + \xi^i \in \mathcal{O}_{\mathbb{K}}$. Mas, $\mathrm{Tr}(x(1-\xi)) \in \mathcal{O}_{\mathbb{K}} \cap \mathbb{Q} = \mathbb{Z}$. Portanto, $\mathrm{Tr}(x(1-\xi)) \in \mathcal{O}_{\mathbb{K}}(1-\xi) \cap \mathbb{Z} = \mathbb{Z}p$, e assim $a_0 \in \mathbb{Z}$. Agora, para mostrar que $a_1, a_2, \cdots, a_{p-2}$ também pertencem a $\mathbb{Z}$, usamos indução. Para mostrar que $a_j \in \mathbb{Z}$ multiplicamos a Equação (1.4) por ξ^{p-j} e obtemos

$$x\xi^{p-j} = a_0\xi^{p-j} + a_1\xi^{p-j-1} + \cdots + a_{j-1}\xi^{p-1} + a_j + a_{j+1}\xi + \cdots + a_{p-2}\xi^{p-j-2}. \tag{1.7}$$

Expressando ξ^{p-1} em termos das potências menores de ξ, podemos escrever $x\xi^{p-j}$ na forma

$$x\xi^{p-j} = (a_j - a_{j-1}) + a'_1\xi + a'_2 + \cdots + a'_{p-2}. \tag{1.8}$$

Por hipótese de indução, $a_{j-1} \in \mathbb{Z}$ e com o mesmo argumento tem-se que $a_j - a_{j-1} \in \mathbb{Z}$. Portanto, $a_j \in \mathbb{Z}$. Assim, tem-se que $\{1, \xi, \xi^2, \cdots, \xi^{p-2}\}$ é uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{K}}$, e além disso, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi]$. □

1.6 Norma de um ideal

Nesta seção, definimos a norma de um ideal de $\mathcal{O}_{\mathbb{K}}$ e exibimos algumas de suas propriedades que serão úteis no decorrer dos próximos capítulos. As principais referências usadas nesta seção são [1],[4] e [2].

Definição 1.6.1. *Seja A um domínio de integridade que não é um corpo, e $\mathbb{K}$ o seu corpo de frações. Um A-submódulo $\mathfrak{b}$ de $\mathbb{K}$ é chamado de ideal fracionário de A, se existir $d \in A - 0$ tal que $d\mathfrak{b} \subset A$. Os ideais de A são chamados de ideais inteiros.*

Definição 1.6.2. *Um anel A é dito ser Noetheriano se satisfaz umas das seguintes condições:*

1. *Todo conjunto não vazio de ideais de A contém um elemento maximal.*
2. *Todo sequência crescente de ideais de A é estacionaria.*
3. *Todo ideal de A é finitamente gerado.*

Definição 1.6.3. *Dizemos que um anel A é um anel de Dedekind, se satisfaz as seguintes condições:*

1. *A é integralmente fechado.*
2. *A é Noetheriano.*
3. *Todo ideal não nulo de A é maximal.*

Definição 1.6.4. *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros algébricos de $\mathbb{K}$. Se $\mathfrak{a}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, definimos a norma do ideal $\mathfrak{a}$ com sendo a cardinalidade do anel quociente de $\mathcal{O}_{\mathbb{K}}$ por $\mathfrak{a}$, isto é,*

$$N(\mathfrak{a}) = card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right).$$

Definição 1.6.5. *Sejam A um anel, $\mathfrak{m}$ um ideal maximal de A e B um A-módulo. Dizemos que B é anulado por $\mathfrak{m}$ quando para todo $m \in \mathfrak{m}$ e $b \in B$, tem se que $mb = 0$.*

Se B é um A-módulo anulado por um ideal maximal $\mathfrak{m}$, então B pode ser considerado como um $\frac{A}{\mathfrak{m}}$ espaço vetorial. Assim, podemos estabelecer o seguinte resultado.

Lema 1.6.1. *Se A é um domínio de Dedekind, $\mathfrak{m}$ um ideal maximal de A e $\mathfrak{b}$ um ideal não nulo de A, então $\frac{\mathfrak{b}}{\mathfrak{mb}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial de dimensão* 1.

Demonstração: Se $\overline{x} \in \frac{\mathfrak{b}}{\mathfrak{mb}}$, então $\overline{x} = x + \mathfrak{mb}$, onde $x \in \mathfrak{b}$. Assim, se $m \in \mathfrak{m}$, então $m\overline{x} = mx + \mathfrak{mb}$. Logo, $m\overline{x} \in \mathfrak{mb}$, ou seja, $\frac{\mathfrak{b}}{\mathfrak{mb}}$ é anulado por $\mathfrak{m}$. Portanto, $\frac{\mathfrak{b}}{\mathfrak{mb}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial. Os $\frac{A}{\mathfrak{m}}$-subespaços próprios de $\frac{\mathfrak{b}}{\mathfrak{mb}}$ são da forma $\frac{\mathfrak{q}}{\mathfrak{mb}}$, onde $\mathfrak{q}$ é um ideal tal que $\mathfrak{mb} \subsetneq \mathfrak{q} \subsetneq \mathfrak{b}$ o que não pode ocorrer, portanto $\frac{\mathfrak{b}}{\mathfrak{mb}}$ é um $\frac{A}{\mathfrak{m}}$-espaço vetorial de dimensão 1. □

Teorema 1.6.1. *Seja A um domínio Dedekind que não é um corpo. Se $\wp$ é o conjunto de todos os ideais primos não nulos de A, então todo ideal fracionário $\mathfrak{p}'$ não nulo de A pode ser expresso como o produto de potências de ideais primos de A de modo único, isto é,*

$$\mathfrak{p}' = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i}$$

onde $e_1, \cdots, e_n \in \mathbb{Z}$.

Demonstração: Mostramos inicialmente a existência da decomposição. Se $\mathfrak{p}'$ é um ideal fracionário de A, então existe $d \in A - 0$ tal que $d\mathfrak{b}' \subset A$. Logo, $d\mathfrak{b}'$ é um ideal inteiro de A, e assim escrevendo $d\mathfrak{p}' = Ad\mathfrak{p}'$ tem-se que $\mathfrak{p}' = (Ad)^{-1}(d\mathfrak{p}')$. Se mostrarmos que $Ad = \prod_{i=1}^{n} \mathfrak{p}_i^{r_i}$ e que $d\mathfrak{p}' = \prod_{i=1}^{n} \mathfrak{p}_i^{s_i}$, com $r_i, s_i \in \mathbb{Z}$, então $\mathfrak{p}' = \prod_{i=1}^{n} \mathfrak{p}_i^{s_i - r_i}$. Assim, é suficiente mostrarmos o resultado para ideais inteiros de A. Seja $\wp$ a família dos ideais inteiros de A, não nulos, que não são o produto de potências de ideais primos de A, E suponhamos que $\wp \neq \emptyset$, como A é noetheriano, segue que $\wp$ tem um elemento maximal $\mathfrak{m}$, e $\mathfrak{m} \neq A$, uma vez que A é o produto da coleção vazia de ideais primos, logo, $\mathfrak{m} \subseteq \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal maximal de A. Além disso, $\mathfrak{q} = \{x \in \mathbb{K};\, x\mathfrak{p} \subset A\}$ é tal que $\mathfrak{pq} = A$. Como $\mathfrak{m} \subseteq \mathfrak{p}$, segue que $\mathfrak{mq} \subseteq \mathfrak{pq} = A$. Além disso, como $A \subset q$, segue que $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{mq} \subset A$. Assim, $\mathfrak{m} \subsetneq \mathfrak{mq}$, pois se $\mathfrak{m} = \mathfrak{mq}$ e se $x \in \mathfrak{q}$, então $x\mathfrak{m} \subset \mathfrak{m}$. Logo, $x^n\mathfrak{m} \subset \mathfrak{m}$ para todo $n \in \mathbb{N}$, e assim se $d \in \mathfrak{m} - 0$, então $dx^n \in \mathfrak{m} \subseteq A$. Portanto, $A[x]$ é um ideal fracionário de A. Como A é neotheriano, segue que $A[x]$ é um A-módulo finitamente gerado, e assim x é inteiro sobre A. Agora, como A é integralmente fechado, segue que $x \in A$, e portanto, $\mathfrak{q} \subset A$. Assim, $\mathfrak{q} = A$, mas isto não pode ocorrer uma vez que se $\mathfrak{q} = A$, então $\mathfrak{p} = \mathfrak{p}A = \mathfrak{pq} = A$ o que é um absurdo, pois $\mathfrak{p}$ é um ideal primo. Pela maximalidade de $\mathfrak{m}$ e como $\mathfrak{m} \subseteq \mathfrak{mq}$, segue que $\mathfrak{mq} \nsubseteq \wp$, ou seja, $\mathfrak{mq} = \prod_{i=1}^{n} p_i^{e_i}$, onde $p_i,\ \ i = 1, 2, \cdots, n$ são ideais primos de A. Multiplicando ambos os lados por $\mathfrak{p}$, segue que

$$(\mathfrak{mq})\mathfrak{p} = \mathfrak{m}(\mathfrak{pq}) = \mathfrak{m}A = \mathfrak{m} = \prod_{i=1}^{n} p_i^{e_i}\mathfrak{p}$$

o que é um absurdo, pois $\mathfrak{m} \in \wp$. Portanto, $\wp = \emptyset$, e assim concluímos a prova da existência. Para a unicidade, suponhamos que $\mathfrak{p}$ seja um ideal inteiro de A que admite duas fatorações distintas em ideais primos, ou seja,

$$\mathfrak{p} = \prod_{i=1}^{n} \mathfrak{p}^{n_i} \qquad \text{e} \qquad \mathfrak{p} = \prod_{i=1}^{n} \mathfrak{p}^{m_i},$$

com $m_i \neq n_i$ para algum $i \in \mathbb{N}$. Assim, $\prod_{\mathfrak{p}_i \in \wp} \mathfrak{p}^{n_i - m_i} = A$. Denotamos por $-\beta = n_i - m_i$ se $n_i < m_i$ e por $\alpha = n_i - m_i$ se $n_i > m_i$. Assim,

$$\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2}\cdots\mathfrak{q}_s^{\beta_s},$$

onde $\mathfrak{p}_i, \mathfrak{q}_j \in \wp$ e $\mathfrak{p}_i \neq \mathfrak{q}_j$, com $i = 1, 2, \cdots, r$ e $j = 1, 2, \cdots, s$. Como $\mathfrak{p}_1$ é primo e $\mathfrak{p}_1 \supseteq \mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2}\cdots\mathfrak{q}_s^{\beta_s}$, segue que $\mathfrak{p}_1 \supseteq \mathfrak{q}_j$ para algum $j = 1, 2, \cdots, s$. Fazendo uma reordenação, se necessário, podemos supor que $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$. Assim, $\mathfrak{p}_1 = \mathfrak{q}_1$ uma vez que $\mathfrak{q}_1$ é maximal, o que contrária o fato de que $\mathfrak{p}_i \neq \mathfrak{q}_j$ para $i = 1, 2, \cdots, r$ e $j = 1, 2, \cdots, s$. Portanto, a fatoração é única. □

Proposição 1.6.1. *Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Demonstração: Uma vez que o ideal $\mathfrak{b}$ se fatora em produto de ideias primo, é suficiente mostrarmos que $\mathrm{N}(\mathfrak{am}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{m})$ para $\mathfrak{m}$ um ideal primo. Consideremos o homomorfismo

$$\begin{aligned}\phi &: \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}} \to \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}} \\ \phi &\ (x + \mathfrak{am}) = x + \mathfrak{a}.\end{aligned}$$

Uma vez que $\mathfrak{am} \subset \mathfrak{a}$, segue que ϕ é sobrejetora, e além disso, $Ker(\phi) = \frac{\mathfrak{a}}{\mathfrak{am}}$. Logo,

$$card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{am}}\right) = card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right) card\left(\frac{\mathfrak{a}}{\mathfrak{am}}\right).$$

Assim, devemos mostrar que $card\left(\frac{\mathfrak{a}}{\mathfrak{am}}\right) = card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}\right)$. Agora, $\frac{\mathfrak{a}}{\mathfrak{am}}$ é um $\mathcal{O}_{\mathbb{K}}$-módulo anulado por $\mathfrak{m}$, o que significa que podemos considera-lo como um espeço vetorial sobre $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}$. Estes subespaços possuem submódulos que são da forma $\frac{\mathfrak{q}}{\mathfrak{am}}$, onde $\mathfrak{q}$ é um ideal tal que $\mathfrak{am} \subset \mathfrak{q} \subset \mathfrak{a}$. Mas, como não existem ideais entre $\mathfrak{am}$ e $\mathfrak{a}$, segue pelo Lema 1.6.1 que o espaço vetorial $\frac{\mathfrak{a}}{\mathfrak{am}}$ tem dimensão 1 sobre $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}$, o que implica que

$$card\left(\frac{\mathfrak{a}}{\mathfrak{am}}\right) = card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{m}}\right),$$

provando a proposição. □

Proposição 1.6.2. *Se $\mathfrak{b}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{b}) \in \mathfrak{b}$.*

Demonstração: O conjunto $\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{b}}$ é um grupo aditivo tal que $card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{b}}\right) = \mathrm{N}(\mathfrak{b})$. Assim, $\mathrm{N}(\mathfrak{b})\overline{1} = \overline{0}$, ou seja, $\mathrm{N}(\mathfrak{b}) \in \mathfrak{b}$. □

Proposição 1.6.3. *Seja $\mathfrak{b}$ um ideal de $\mathcal{O}_{\mathbb{K}}$. Se $N(\mathfrak{b})$ é um número primo, então $\mathfrak{b}$ é um ideal primo.*

Demonstração: Suponhamos que $\mathfrak{b}$ não seja um ideal primo de $\mathcal{O}_{\mathbb{K}}$. Assim, $\mathfrak{b} = \mathcal{O}_{\mathbb{K}}$ ou então $\mathfrak{b} = \mathfrak{a}\mathfrak{m}$, onde $\mathfrak{a}$ e $\mathfrak{m}$ são ideais não nulos e distintos de $\mathcal{O}_{\mathbb{K}}$. No primeiro caso, tem-se que $\mathrm{N}(\mathfrak{b}) = 1$, e no segundo caso tem-se que $\mathrm{N}(\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{m})$. Em ambos os casos concluímos que $\mathrm{N}(\mathfrak{b})$ não é um número primo, o que contradiz a hipótese, portanto devemos ter que $\mathfrak{b}$ é um ideal primo. □

Proposição 1.6.4. *Se $\mathfrak{b}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(\mathfrak{b}) = 1$ se, e somente, se $\mathfrak{b} = \mathcal{O}_{\mathbb{K}}$.*

Demonstração: Por definição tem-se que $\mathrm{N}(\mathfrak{b}) = 1$ se, e somente se, $card\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{b}}\right) = 1$ se, e somente se, $\mathcal{O}_{\mathbb{K}} = \mathfrak{b}$. □

Definição 1.6.6. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ uma base para $\mathbb{K}$ como um $\mathbb{Q}$-espaço vetorial. O discriminante desta base é definido como*

$$\Delta[\alpha_1, \alpha_2, \cdots, \alpha_n] = \det[\sigma_i(\alpha_j)]^2.$$

Se tomarmos uma outra base $\{\beta_1, \beta_2, \cdots, \beta_n\}$ de $\mathbb{K}$, então

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i, \text{ com } c_{ik} \in \mathbb{Q}, \text{ para } k = 1, 2, \cdots, n,$$

e que $\det c_{ik} \neq 0$. Uma vez que os σ_i's são $\mathbb{K}$-automorfismo, tem-se que

$$\begin{aligned}
\Delta[\beta_1, \beta_2, \cdots, \beta_n] = \det(\sigma_i(\beta_j))^2 &= \det(\sigma_i(\sum_{i=1}^{n} c_{ik}\alpha_i))^2 \\
&= \det(\|c_{ik}\| \, \|\sigma_i(\alpha_i)\|)^2 \\
&= \det(c_{ik})^2 \det(\sigma_i(\alpha_i))^2 \\
&= \det(c_{ik})^2 \Delta[\alpha_1, \alpha_2, \cdots, \alpha_n].
\end{aligned}$$

Teorema 1.6.2. *Sejam G um grupo abeliano livre de rank r e H um subgrupo de G. Assim, G/H tem rank finito se, e somente, se o rank de G e H são iguais. Além disso, se G e H tem $\mathbb{Z}$-bases $\{x_1, x_1, \cdots, x_n\}$ e $\{y_1, y_1, \cdots, y_n\}$, respectivamente, com $y_i = \sum_j a_{ij}x_j$, então $\mid G/H \mid = \mid \det(a_{ij}) \mid$.*

Demonstração: Ver [2], pg. 30. □

Teorema 1.6.3. *Se $\mathbb{K}$ é um corpo de números com $\mathcal{O}_\mathbb{K}$ o seu anel dos inteiros algébricos, então todo ideal $\mathfrak{a}$ não nulo de $\mathcal{O}_\mathbb{K}$ possui uma $\mathbb{Z}$-base $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, onde n é o grau do corpo de números $\mathbb{K}$, e*

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \alpha_2, \cdots, \alpha_n]}{\Delta} \right|^{\frac{1}{2}},$$

onde Δ é o discriminante do corpo $\mathbb{K}$.

Demonstração: O conjunto $(\mathcal{O}_\mathbb{K}, +)$ é um grupo abeliano livre de rank n. Como $\frac{\mathcal{O}_\mathbb{K}}{\mathfrak{a}}$ tem rank finito, segue que $(\mathfrak{a}, +)$ é um grupo abeliano de rank n, e portanto possui uma $\mathbb{Z}$-base da forma $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$. Agora, se $\{w_1, w_2, \cdots, w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_\mathbb{K}$ e se $\alpha_i = \sum_j c_{ij}w_j$, então pelo Teorema 1.6.2 segue que

$$\mathrm{N}(\mathfrak{a}) = \left| \frac{\mathcal{O}_\mathbb{K}}{\mathfrak{a}} \right| = \det(c_{ij}).$$

Agora, como $\Delta[w_1, w_2, \cdots, w_n] = \det(c_{ij})^2\Delta$, segue que se $\Delta[w_1, w_2, \cdots, w_n] = \mathrm{N}(\mathfrak{a})^2\Delta$, então $\mathrm{N}(\mathfrak{a}) = \left| \frac{\Delta[w_1, w_2, \cdots, w_n]}{\Delta} \right|^{\frac{1}{2}}$. □

Corolário 1.6.1. *Se $\mathfrak{p} = \langle a \rangle$ é um ideal principal de $\mathcal{O}_\mathbb{K}$, então $N(\mathfrak{a}) = \mid N(a) \mid$.*

Demonstração: Segue diretamente do Teorema 1.6.3. □

1.7 Classe de ideais

Nessa seção, definimos o conceito de classe de ideais e o número de classes que serão amplamente usados no Capítulo 3. A principal referência para essa seção é [1].

Sejam $\{x_1, x_2, \cdots, x_n\}$ uma base integral de um corpo $\mathbb{K}$, e $x_i^{(1)}, x_i^{(2)}, \cdots, x_i^{(n)}$ os conjugados de x_i. Se

$$\mu = \prod_{j=1}^{n} \sum_{i=1}^{n} \mid x_i^{(j)} \mid,$$

então μ é um número real positivo .

Lema 1.7.1. *Se $\mathbb{K}$ é um corpo de números, então para todo ideal inteiro $\mathfrak{J}$ de $\mathcal{O}_{\mathbb{K}}$, existe um elemento $a \in \mathfrak{J}$, com $a \neq 0$, tal que $\mid N_{K\mid\mathbb{Q}}(a) \mid \leq N(\mathfrak{J})\mu$.*

Demonstração: Ver [1], pg. 144. □

Se $\mathfrak{F}$ é o grupo multiplicativo abeliano dos ideais fracionários não nulos de $\mathcal{O}_{\mathbb{K}}$ e $\wp_r$ é o subgrupo dos ideais fracionários principais não nulos, então podemos considerar o grupo quociente $\frac{\mathfrak{F}}{\wp_r}$. Dois ideais fracionários não nulos, M e M' são ditos serem equivalentes, quando existe $x \in \mathbb{K}$, com $x \neq 0$, tal que $M' = \mathcal{O}_{\mathbb{K}} x M$, onde denotamos por $M \sim M'$. Tal relação é claramente de equivalência e se $M_1 \sim M_2$ e $M_1' \sim M_2'$, então $M_1 M_1' \sim M_2 M_2'$. Além disso, $\wp_r$ é precisamente o subgrupo cujos os ideais são equivalentes ao ideal unidade de $\mathcal{O}_{\mathbb{K}}$. Cada elemento de $\frac{\mathfrak{F}}{\wp_r}$ é chamado uma *classe de ideais de* $\mathbb{K}$ e $\frac{\mathfrak{F}}{\wp_r}$ é chamado *grupo das classes de ideais de* $\mathbb{K}$ que denotamos por $Cl_{\mathbb{K}}$.

Uma questão natural que se coloca é que será possível que $\frac{\mathfrak{F}}{\wp_r}$ tenha índice infinito? No próximo teorema, respondemos essa questão para corpos de números algébricos.

Teorema 1.7.1. *O número de classes de ideais de um corpo de números é finito.*

Demonstração: A norma de um ideal inteiro é um inteiro positivo. Assim, para o número real μ, segue que existe somente um número finito de ideais não nulos $\mathfrak{J}_1, \mathfrak{J}_2, \cdots, \mathfrak{J}_k$ tal que $\mathrm{N}(\mathfrak{J}_i) \leq \mu$. Assim, mostramos que se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então I é equivalente a algum ideal $\mathfrak{J}_i$ e assim o número de classes de ideais não é maior do que k e

portanto finito. Agora, se I^{-1} é o ideal fracionário inverso de I, então existe um elemento $c \in \mathcal{O}_{\mathbb{K}}$, com $c \neq 0$, tal que cI^{-1} é um ideal inteiro. Pelo Lema 1.7.1, segue que existe um elemento $b \in cI^{-1}$, com $b \neq 0$, tal que $\mathrm{N}(\mathcal{O}_{\mathbb{K}}b) \leq \mathrm{N}(cI^{-1})\mu$. Multiplicando por $\mathrm{N}(I)$ e observando que $Ibc^{-1} \subseteq \mathcal{O}_{\mathbb{K}}$ obtém-se que

$$\mathrm{N}(Ibc^{-1})\mathrm{N}(\mathcal{O}_{\mathbb{K}}c) = \mathrm{N}(Ibc^{-1}\mathcal{O}_{\mathbb{K}}c) = \mathrm{N}(Ib) = \mathrm{N}(\mathcal{O}_{\mathbb{K}}b)\mathrm{N}(I) \leq \mathrm{N}(cI^{-1})\mathrm{N}(I)\mu = \mathrm{N}(\mathcal{O}_{\mathbb{K}}c)\mu.$$

Assim, $\mathrm{N}(Ibc^{-1}) \leq \mu$, e portanto $Ibc^{-1} = \mathfrak{J}_i$ para algum índice i. Logo, $I \sim \mathfrak{J}_i$ para algum índice i, o que conclui a demonstração. □

Definição 1.7.1. *O número das classes de ideais de um corpo de números algébricos* $\mathbb{K}$ *é chamado de classe de números de* $\mathbb{K}$ *e é denotado por* $h = h_{\mathbb{K}}$.

Proposição 1.7.1. *Se* $\mathfrak{J}$ *é um ideal fracionário não nulo do anel* $\mathcal{O}_{\mathbb{K}}$, *então* $\mathfrak{J}^h$ *é um ideal fracionário principal de* $\mathcal{O}_{\mathbb{K}}$.

Demonstração: Como h é a ordem do grupo multiplicativo $\frac{\mathfrak{F}}{\wp_r}$ das classes dos ideais de $\mathbb{K}$, segue que a h-ésima potência de todo ideal fracionário é um ideal principal, pois se $\mathfrak{J} \in \frac{\mathfrak{F}}{\wp_r}$, então $\mathfrak{J}^h = \overline{1}$. Assim, $\mathfrak{J}^h \in \wp_r$. □

1.8 Considerações finais do capítulo

O Capítulo 1, tem como objetivo expor alguns resultados que servirão de base teórica para o desenvolvimento dos demais capítulos. Destacamos neste capítulo a importância da Seção (1.2), onde trabalhamos o conceito de elementos inteiros e da Seção (1.4), onde trabalhamos o conceito de traço e norma de um elemento, que serão importantes para caracterizar as unidades de um anel de inteiros.

Capítulo 2

Unidades corpos de números

Nesse capítulo, apresentamos alguns resultados que serão necessários para a demonstração do Teorema das unidades de Dirichlet, que diz que num corpo de números $\mathbb{K}$ de grau n o anel de inteiros $\mathcal{O}_{\mathbb{K}}$ é o produto de um grupo cíclico finito (a saber, o grupo das raízes da unidade contidas em $\mathbb{K}$) por um $\mathbb{Z}$-módulo livre de posto $r = r_1+r_2-1$, onde r_1 é o número de imersões reais e $2r_2$ é o número de imersões puramente complexas de $\mathbb{K}$. Na Seção (2.1), mostramos que o grupo das raízes da unidade de $\mathbb{K}$ é um grupo multiplicativo cíclico finito e daremos a caracterização das unidades de $\mathcal{O}_{\mathbb{K}}$. Na Seção (2.2), apresentamos as unidades do anel de inteiros de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ com $d < 0$ livre de quadrados, e apresentamos o conceito de unidade fundamental. Na Seção (2.3), apresentamos as unidades do anel de inteiros de um corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\xi_p)$, onde ξ_p é uma raiz p-ésima primitiva da unidade e p um número primo. Na Seção (2.4), apresentamos alguns resultados que auxiliam na demonstração do Teorema de Dirichlet e definimos o regulador de $\mathbb{K}$.

2.1 Unidades

Nesta seção, apresentamos as unidades de um corpo de números $\mathbb{K}$, onde estabelecemos a relação entre as unidades de $\mathcal{O}_{\mathbb{K}}$ e as raízes da unidade de $\mathbb{K}$. Apresentamos, também, uma caracterização das raízes da unidade (Proposição 2.1.5), onde as principais referências

desta seção são [1] e [2].

Proposição 2.1.1. *Toda raiz da unidade em $\mathbb{K}$ é uma unidade em $\mathcal{O}_{\mathbb{K}}$.*

Demonstração: Se $z \in \mathbb{K}$ é uma raiz da unidade, então existe $n \in \mathbb{N}$, tal que $z^n - 1 = 0$. Assim, z é uma raiz de $x^n - 1$, e deste modo, $z \in \mathcal{O}_{\mathbb{K}}$. Além disso, z é uma unidade de $\mathcal{O}_{\mathbb{K}}$ uma vez que $zz^{n-1} = z^n = 1$, e assim, $z^{n-1} \in \mathcal{O}_{\mathbb{K}}^*$. □

Denotamos por U o grupo das unidades de $\mathcal{O}_{\mathbb{K}}$, e por W o grupo das raízes da unidade em $\mathbb{K}$. Assim, pela Proposição 2.1.1, segue que $W \subseteq U$. Notemos que 1 e -1 são elementos de W. Assim, $W \neq \phi$, e portanto, $U \neq \phi$.

Observação 2.1.1. *Para a próxima proposição usamos o seguinte resultado. Se $f(x)$ é um polinômio de grau n sobre $\mathbb{K}$ com raízes $r_1, r_2, \cdots, r_n$ e se $p(x_1, x_2, \cdots, x_n)$ é um polinômio simétrico sobre $\mathbb{K}$, então $p(r_1, r_2, \cdots, r_n) \in \mathbb{K}$ (uma demonstração para esta observação pode ser encontrada em [4]).*

Proposição 2.1.2. *Se $c \in \mathbb{Z}$ é positivo e $\mathbb{K}$ é um corpo de números, então existe somente um número finito de inteiros algébricos $x \in \mathbb{K}$, tal que $|x^{(i)}| \leq c$, para todo conjugado $x^{(i)}$ de x.*

Demonstração: Primeiro, determinamos um conjunto finito S que depende apenas de c, e provamos que se $x \in \mathcal{O}_{\mathbb{K}}$ é tal que $|x^{(i)}| \leq c$ para todo conjugado $x^{(i)}$, então $x \in S$. Para isso, sejam $[\mathbb{K} : \mathbb{Q}] = n$ e $s_1, s_2, \cdots, s_n$ os polinômios simétricos elementares em n variáveis, isto é,

$$\begin{cases} s_1 = x_1 + x_2 + \cdots + x_n \\ s_2 = \sum_{i<j} x_i x_j \\ \vdots \\ s_n = x_1 x_2 \cdots x_n \end{cases}$$

Seja c' um número real suficientemente grande, por exemplo,

$$c' = max\left\{nc, \left(\frac{n}{2}\right)c^2, \cdots, \left(\frac{n}{k}\right)c^k, \cdots, c^n\right\}.$$

Aqui, $\binom{n}{i}$ denota a combinação de n elementos tomados i a i. Seja F o conjunto de todos os polinômios mônicos de grau no máximo n cujos os coeficientes são inteiros a_i tal que $|a_i| \leq c'$, isto é,

$$F = \{a_0 + a_1 x + \cdots + x^r;\ \ r \leq n;\ |a_i| \leq c',\ i = 0, 1, \cdots, n\}.$$

O conjunto F é finito, uma vez que os coeficientes a_i que podemos escolher formam um conjunto finito. Agora, seja S o conjunto dos elementos de $\mathbb{K}$ que são raízes de algum polinômio pertencente a F, ou seja,

$$S = \{\alpha \in \mathbb{K};\ \text{ existe }\ p(x) \in F \quad \text{tal que},\ \ p(\alpha) = 0\}.$$

O conjunto S é finito uma vez que F é finito. Se $|x^{(i)}| \leq c$ para todo conjugado de $x \in \mathbb{K}$, então $|s_k(x^{(1)}, x^{(2)}, \cdots, x^{(n)})| \leq c'$, para $k = 1, 2, \cdots, n$, uma vez que

$$\begin{cases} |s_1(x^{(1)}, x^{(2)}, \cdots, x^{(n)})| \leq |x^{(1)}| + |x^{(2)}| + \cdots + |x^{(n)}| \leq nc \leq c'. \\ |s_2(x^{(1)}, x^{(2)}, \cdots, x^{(n)})| \leq |\sum x_i x_j| \leq \sum |x_i x_j| \leq \sum c^2 = \binom{n}{2} c^2 \leq c' \\ \vdots \\ |s_n(x^{(1)}, x^{(2)}, \cdots, x^{(n)})| = |x^1||x^2| \cdots |x^n| \leq c^n \leq c'. \end{cases}$$

Como x é um inteiro algébrico, seque que $s_k(x^{(1)}, x^{(2)}, \cdots, x^{(n)}) \in \mathbb{Z}$ para todo $k = 1, 2, \cdots, n$. Porém, $s_k(x^{(1)}, x^{(2)}, \cdots, x^{(n)})$ para todo $k = 1, 2, \cdots, n$, são todos os coeficientes do polinômio $\rho(x) = \prod(x - x^i)$. Logo, $\rho(x) \in \mathbb{Z}[x]$ possui os coeficientes s_k limitados, e portanto, $\rho(x) \in F$. Assim, $x \in S$ uma vez que x é uma raiz de $\rho(x)$. $\square$

Um corolário imediato do resultado da Proposição 2.1.2 é uma caracterização das raízes da unidade em $\mathbb{K}$.

Proposição 2.1.3. *Um elemento $x \in \mathbb{K}$ é uma raiz da unidade, 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 $x \in \mathbb{K}$ é uma raiz da unidade, então o mesmo ocorre com todo conjugado $x^{(i)} = \sigma_{(i)}(x)$, pois, se $x^n = 1$ então $\sigma_i(x)^n = \sigma_i(x^n) = \sigma_i(1) = 1$. Logo,

$$|\ x^{(i)}\ |^n = |\ x^{(i)n}\ | = |\ 1\ | = 1 \Rightarrow |\ x^{(i)}\ | = (|\ x^{(i)}\ |^n)^{\frac{1}{n}} = 1^{\frac{1}{n}} = 1,$$

para todo i. Reciprocamente, suponhamos que x é um inteiro algébrico de $\mathbb{K}$ tal que $\mid x^{(i)} \mid = 1$ para todo conjugado $x^{(i)}$ de x. Pela Proposição 2.1.2, segue que existe somente um número finito de inteiros algébrico $y \in \mathbb{K}$ tal que $\mid y^{(i)} \mid = 1$ para todo conjugado $y^{(i)}$ de y. Porém as potencias, $y, y^2, y^3 \cdots$, satisfazem a esta propriedade uma vez que $y^k \in \mathcal{O}_{\mathbb{K}}$ e

$$\mid y^{k^{(i)}} \mid = \mid \sigma_{(i)}(y^k) \mid = \mid \sigma_{(i)}(y)^k \mid = \mid \sigma_{(i)}(y) \mid^k = \mid y^{(i)} \mid^k = \mid 1 \mid = 1.$$

Assim, o conjunto $\{y, y^2, y^3, \cdots\}$ deve ser necessariamente finito, e deste modo, existem inteiros r e s distintos, digamos $s < r$, tal que $y^r = y^s$. Logo, $y^r y^{-s} = 1$, ou seja, $y^{r-s} = 1$. Portanto, $y \in \mathbb{K}$ é uma raiz da unidade. □

Proposição 2.1.4. *O grupo W das raízes da unidade em $\mathbb{K}$ é um grupo multiplicativo cíclico finito.*

Demonstração: Claramente W é um subgrupo multiplicativo do grupo U das unidades de $\mathcal{O}_{\mathbb{K}}$. Pelas Proposições 2.1.2 e 2.1.3, segue que W deve ser finito. Se h é o máximo das ordens dos elementos de W, então a ordem de todo elemento de W divide h. Logo, W está contido no grupo das raízes h-ésimas da unidade, uma vez que se $x \in W$ e $o(x) = k$, então $k|h$, ou seja, $h = kr$ para algum $r \in \mathbb{Z}$. Assim, $x^h = (x^k)^r = 1$, ou seja, x é uma raiz h-ésima da unidade. Como o grupo das raízes da unidade é cíclico e é gerado pelos elementos $\{1, \xi_n, \xi_n^2, \cdots, \xi_n^{n-1}\}$, segue que W é cíclico. □

O número de elementos de W será denotado por ω e deve ser par, uma vez que se $x \in W$ então existe $n \in \mathbb{N}$ tal que $x^n = 1$. Assim, $(-x)^{2n} = (x)^{2n} = 1$, ou seja, $-x \in W$.

Proposição 2.1.5. *Um inteiro algébrico x é uma unidade se, e somente se, $N(x) = \pm 1$.*

Demonstração: Se x é uma unidade, então existe um inteiro algébrico x' tal que $xx' = 1$. Assim, $\mathrm{N}(xx') = \mathrm{N}(x)\mathrm{N}(x') = \mathrm{N}(1) = 1$, e deste modo, $\mathrm{N}(x)$ é uma unidade em $\mathbb{Z}$, e portanto, $\mathrm{N}(x) = \pm 1$. Reciprocamente, se $\mathrm{N}(x) = \pm 1$, ou seja, $\mathrm{N}(x) = \prod x^{(i)} = \pm 1$. Assim fazendo $x' = x^{(2)}x^{(3)}, \cdots, x^{(n)}$ segue que $1 = \mathrm{N}(x) = xx'$, e como x' é um inteiro algébrico, segue que x divide 1 em $\mathcal{O}_{\mathbb{K}}$. Portanto, x' é uma unidade em $\mathcal{O}_{\mathbb{K}}$. □

2.2 Unidades em corpos quadráticos

Nesta seção, apresentamos as unidades do anel de inteiros de um corpo quadrático $\mathbb{Q}\left(\sqrt{d}\right)$, e explicitamos as unidades no caso onde d é um inteiro negativo livre de quadrados, e definimos o conceito de unidade fundamental, bem como um método bruto para a determinação das unidades fundamentais de um corpo quadrático. As principais referências desta seção são [1], [2] e [3].

Seja $\mathbb{K} = \mathbb{Q}\left(\sqrt{d}\right)$, onde d é um inteiro racional não nulo e livre de quadrados. Nos próximos resultados, determinamos as unidades de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, para $d < 0$.

Se $d \equiv 2(mod\,4)$ ou $d \equiv 3(mod\,4)$, então os inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ são da forma $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$, e o conjugado de α é dado por $\alpha' = a - b\sqrt{d}$. Assim,

$$\mathrm{N}(\alpha) = \alpha\alpha' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d.$$

Além disso, x é uma unidade se, e somente se, $\mathrm{N}(x) = \pm 1$. Se $d < 0$, então α é uma unidade se, e somente se, $a^2 - b^2 d = 1$.

Agora, se $d \equiv 1(mod\,4)$, então os inteiros algébricos de $\mathbb{Q}(\sqrt{d})$ são da forma $\alpha = \frac{a+b\sqrt{d}}{2}$, com $a, b \in \mathbb{Z}$ e de mesma paridade. Como o conjugado de α é dado por $\alpha' = \frac{a-b\sqrt{d}}{2}$, segue que

$$\mathrm{N}(\alpha) = \alpha\alpha' = \left(\frac{a + b\sqrt{d}}{2}\right)\left(\frac{a - b\sqrt{d}}{2}\right) = \frac{a^2 - b^2 d}{4},$$

segue que α é uma unidade se, e somente se, $\frac{a^2-b^2d}{4} = 1$, ou seja, $a^2 - b^2 d = 4$.

Proposição 2.2.1. *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro racional livre de quadrados.*

1. *Se $d < 0$, $d \neq -1$, $d \neq -3$, então as unidades de $\mathbb{Q}(\sqrt{d})$ são 1 e -1.*
2. *Se $d = -1$, então as unidades de $\mathbb{Q}(\sqrt{-1})$ são $1, -1, i, -i$.*
3. *Se $d = -3$, então as unidades de $\mathbb{Q}(\sqrt{-3})$ são $1, -1, \frac{1\pm\sqrt{-3}}{2}, \frac{-1\pm\sqrt{-3}}{2}$.*

Demonstração: Para o item (1), se $d < 0$, $d \neq -1$ e $d \neq -3$, então devemos considerar dois casos:

a) Se $d' = -d > 0$, então $d' \neq 1$, ou seja, $d' \geq 2$ e $d \neq 3$. Assim, α é uma unidade se, e somente se, $a^2 + b^2 d' = 1$. Como $d' \geq 2$ segue que $b = 0$ e $a = \pm 1$. Logo, $\alpha = 1$ e $\alpha = -1$ são as unidade de $\mathcal{O}_{\mathbb{K}}$.

b) Se $d' = -d > 0$, então $d' \neq 1$. Como $d' \neq 2$ e $d' \neq 3$, segue que $d' \geq 5$ (pois $d' = 4$, não é livre de quadrados). Assim, α é uma unidade se, e somente se, $a^2 + b^2 d' = 4$. Como $d' \geq 5$, segue que $b = 0$ e $a = \pm 1$. Assim, $\alpha = 1$ e $\alpha = -1$, são as unidades de $\mathcal{O}_{\mathbb{K}}$.

Para o item (2), se $d = -1$ então $d \not\equiv 1 (mod\, 4)$. Assim, pelas considerações que precedem este teorema, segue que $\alpha = a + b\sqrt{d}$ é uma unidade se, e somente se, $a^2 + b^2 = 1$. Assim, $a = 0$ e $b = \pm 1$ ou $a = \pm 1$ e $b = 0$, e deste modo, $\alpha = i$, $\alpha = -i$, $\alpha = 1$ e $\alpha = -1$ são as unidades de $\mathcal{O}_{\mathbb{K}}$. Para o item (3), se $d = -3$, então $d \equiv 1 (mod\, 4)$. Assim, das considerações que precederam o teorema, segue que $\alpha = a + b\sqrt{d}$ é uma unidade, se e somente, se $a^2 - b^2 d = 4$, ou seja, $a^2 + 3b^2 = 4$. Portanto, $a = \pm 2$ e $b = 0$ ou $a = \pm 1$ e $b = \pm 1$. Assim, como $\alpha = a + b\sqrt{-3}$, segue que $\alpha = 1$, $\alpha = -1$, $\alpha = \frac{1 \pm \sqrt{-3}}{2}$, $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$ são unidades de $\mathcal{O}_{\mathbb{K}}$. □

Consideraremos, agora, o caso mais interessante, isto é, quando $d > 0$. Neste caso, $\mathbb{Q}(\sqrt{d})$ está contido no corpo dos reais, uma vez que $\sqrt{d} \in \mathbb{R}$. Assim, $\mathbb{Q}(\sqrt{d}) \subset \mathbb{R}$. Deste modo, as raízes da unidade em $\mathbb{Q}(\sqrt{d})$ são 1 e -1. O próximo passo, é analisar as unidades de $\mathcal{O}_{\mathbb{K}}$, onde $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com $d > 0$.

Lema 2.2.1. *Se $\alpha > 0$ é um número irracional, então para todo inteiro racional $m > 0$ existem inteiros racionais a, b não ambos nulos, tais que*

$$| a | \leq m, | b | \leq m \ e \ | a + \alpha b | \leq \frac{1 + \alpha}{m}.$$

Demonstração: Ver [1]. □

Teorema 2.2.1. *Se d é um inteiro positivo livre de quadrados, então o grupo U das unidades do corpo $\mathbb{Q}(\sqrt{d})$ é $U \cong \{1, -1\} \times C$, onde C é um grupo multiplicativo cíclico infinito.*

Demonstração: Tem-se que $W = \{1, -1\}$. Para mostrar a existência de outras unidades em $\mathbb{Q}(\sqrt{d})$, usamos o Lema 2.2.1 com $\alpha = \sqrt{d}$. Para cada inteiro $m > 0$, seja o conjunto

$$S_m = \left\{ (a,b) \in \mathbb{Z} \times \mathbb{Z};\ a^2 + b^2 \neq 0;\ \mid a \mid \leq m,\ \mid b \mid \leq m \text{ e } |a + b\sqrt{d}| \leq \frac{1+\sqrt{d}}{m} \right\}.$$

Pelo Lema 2.2.1, segue que S_m é não vazio, e assim podemos escrever

$$S_m = S_m^+ \cup S_m^- \cup S_m^o,$$

onde

$$\begin{aligned} S_m^+ &= \{(a,b) \in S_m;\ a > 0\} \\ S_m^- &= \{(a,b) \in S_m;\ a < 0\} \\ S_m^o &= \{(a,b) \in S_m;\ a = 0\}. \end{aligned}$$

Note que se $m = 1$, então

$$S_1^o = \{(a,b) \in S_1;\ a = 0\} = \{(0,1), (0,-1)\},$$

e se $m \geq 2$, então $S_m^o = \emptyset$. Afirmamos que $\bigcup_{m \geq 1} S_m$ é um conjunto infinito. De fato, se $\bigcup_{m \geq 1} S_m$ for um conjunto finito, então existe $m_0 \in \mathbb{R}$ tal que

$$\frac{1}{m_0} < |a + b\sqrt{d}|, \quad \forall (a,b) \in \bigcup_{m \geq 1} S_m.$$

No entanto, se m é suficientemente grande e se $(a,b) \in S_m$, então

$$|a + b\sqrt{d}| \leq \frac{1+\sqrt{d}}{m} \leq \frac{1}{m_0},$$

o que é uma contradição. Portanto, $\bigcup_{m \geq 1} S_m$ é infinito, e deste modo $\bigcup_{m \geq 1} S_m^+$ é também infinito. Como $\mid a \mid \leq m$ e $\mid b \mid \leq m$, segue que

$$|a - b\sqrt{d}| \leq |a| + |b\sqrt{d}| \leq |a| + |b|\sqrt{d} \leq m + m\sqrt{d} = m(1 + \sqrt{d}).$$

Além disso,

$$\begin{aligned} 0 \neq |a^2 - b^2 d| = |a^2 - (b\sqrt{d})^2| &= |a - b\sqrt{d}||a + b\sqrt{d}| \\ &\leq m(1+\sqrt{d})(\tfrac{1+\sqrt{d}}{m}) \\ &= (1+\sqrt{d})^2, \end{aligned}$$

para todo $(a,b) \in \bigcup_{m\geq 1} S_m$ e consequentemente, para todo $(a,b) \in \bigcup_{m\geq 1} S_m^+$. Como $|a^2 - b^2 d|$ é um inteiro positivo entre 0 e $(1+\sqrt{d})^2$, segue que existe somente um número finito de possibilidades de valores $a^2 - b^2 d$, para $(a,b) \in \bigcup_{m\geq 1} S_m^+$. Como $\bigcup_{m\geq 1} S_m^+$ é infinito, segue que existe um inteiro n tal que $n = a^2 - b^2 d$, com $0 < |n| < (1+\sqrt{d})^2$, para um número infinito de pares (a,b) com $a > 0$. Além disso, tem-se que

$$(a_1, b_1) \equiv (a_2, b_2) \Longleftrightarrow a_1 \equiv a_2 \,(mod\ n) \text{ e } \ b_1 \equiv b_2 \,(mod\ n)$$

é uma relação de equivalência. Entre os infinitos pares de elementos (a,b), com $a > 0$ para os quais existe n tal que $0 < |n| < (1+\sqrt{d})^2$ e $n = a^2 - b^2 d$, consideramos $n^2 + 1$ dentre eles, de modo que tenhamos no máximo n^2 classes de equivalência. Sejam $x_1 = a_1 + b_1\sqrt{d}$ e $x_2 = a_2 + b_2\sqrt{d}$ dois elementos distintos numa mesma classe de equivalência e considere $u = \frac{x_1}{x_2}$. Assim, $\mathrm{N}(x_1) = (a_1 + b_1\sqrt{d})(a_1 - b_1\sqrt{d}) = a_1^2 - b_2^2 d = n$ e $\mathrm{N}(x_2) = (a_2 + b_2\sqrt{d})(a_2 - b_2\sqrt{d}) = a_1^2 - b_2^2 d = n$. Deste modo, $\mathrm{N}(u) = 1$ e $u \neq 1$, pois $x_1 \neq \pm x_2$, uma vez que $(a_1, b_1) \neq (a_2, b_2)$ e $a_1, a_2 > 0$. Além disso,

$$\begin{aligned} u &= \tfrac{x_1}{x_2} = 1 + \tfrac{x_1 - x_2}{x_2} = 1 + \tfrac{(x_1 - x_2)x_2'}{\mathrm{N}(x_2)} \\ &= 1 + \tfrac{(a_1 - a_2) + (b_1 - b_2\sqrt{d})}{n}(a_2 - b_2\sqrt{d}), \end{aligned}$$

onde x_2' denota o conjugado de x_2, fazendo

$$a' = \frac{a_1 - a_2}{n} \text{ e } b' = \frac{b_1 - b_2}{n}, \ \text{ com } \ a', b' \in \mathbb{Z},$$

segue que

$$u = 1 + (a' + b'\sqrt{d})(a_2 - b_2\sqrt{d}) = (1 + a'a_2 - b'b_2 d) + (a_2 b' - a'b_2)\sqrt{d}$$

é um inteiro algébrico. Como $\mathrm{N}(u) = 1$, segue que u é uma unidade e como vimos é diferente de 1 e -1. Logo, existe ao menos uma unidade $u > 1$ em $\mathbb{Q}(\sqrt{d})$, uma vez

que se u é uma unidade, então $-u, u^{-1}, -u^{-1}$ são também unidades e ao menos uma delas é maior do que 1. Agora, provamos que entre as unidades $u > 1$ existe uma menor possível. Com efeito, se u é uma unidade tal que $u > 1$ e se $c \in \mathbb{R}$ é tal que $1 < u < c$, então $\mathrm{N}(u) = \pm 1$. Se $\mathrm{N}(u) = uu' = 1$, então $\frac{1}{c} < u' < 1$. Agora, se $\mathrm{N}(u) = -1$, então $-1 < u' < -\frac{1}{c}$. Assim, segue que $\frac{1}{c} < u' < 1$ ou $-1 < u' < -\frac{1}{c}$ e em qualquer caso, tem-se que $\mid u' \mid \leq c$. Pela Proposição 2.1.2, segue que existe somente um número finito de inteiros algébricos u_i tal que $\mid u_i' \mid < c$. Assim, o conjunto de tais unidades é finito, e deste modo, admite um elemento mínimo, ou seja, existe u sendo a menor unidade tal que $u > 1$. Seja u_1 a menor unidade tal que $u_1 > 1$. Agora, provamos que toda unidade positiva é uma potência de u_1. Com efeito, se $u > 0$ é uma unidade, então existe $m \in \mathbb{Z}$ tal que $u_1^m \leq u < u_1^{m+1}$ assim, $\frac{u}{u_1^m}$ é também uma unidade tal que $1 \leq \frac{u}{u_1^m} < u_1$. Como u_1 é a menor unidade maior que 1, segue que $\frac{u}{u_1^m} = 1$, e portanto, $u = u_1^m$. Similarmente, toda unidade negativa é da forma $-u^m$ para algum $m \in \mathbb{Z}$. Sejam C o grupo gerado por u_1. A aplicação $\varphi : U \longrightarrow \{1, -1\} \times C$, definida por

$$\varphi(u_1^m) = (1, u_1^m)$$
$$\varphi(-u_1^m) = (1, -u_1^m)$$

é um isomorfismo, e portanto,

$$U \cong \{1, -1\} \times C,$$

o que prova o teorema. □

Definição 2.2.1. *A menor unidade $u_1 > 1$ de $\mathcal{O}_{\mathbb{K}}$ é chamada de unidade fundamental do corpo $\mathbb{K}$.*

Exemplo 2.2.1. *Em $\mathbb{Q}(\sqrt{2})$ não existe uma unidade entre 1 e $1 + \sqrt{2}$. De fato, se $\epsilon = x + y\sqrt{2}$ é uma unidade entre 1 e $1 + \sqrt{2}$, então*

$$N(\epsilon) = x^2 - 2y^2 = \pm 1$$

e

$$1 < \epsilon < 1 + \sqrt{2}. \tag{2.1}$$

Assim, $N(\epsilon) = x^2 - 2y^2 = (x+y\sqrt{2})(x-y\sqrt{2}) = \pm 1$ *se, e somente se,* $x - y\sqrt{2} = \frac{\pm 1}{x+y\sqrt{2}} < 1$ *e*

$$|x - y\sqrt{2}| < 1. \tag{2.2}$$

Somando as desigualdades (2.1) e (2.2) membro a membro, segue que $0 < 2x < 2 + 2\sqrt{2}$*, ou seja,* $0 < x < 1,8$*. Uma vez que* $x \in \mathbb{Z}$*, segue que* $x = 1$*. Mas,*

$$1 < 1 + y\sqrt{2} < 1 + \sqrt{2}$$

não é possível para nenhum valor inteiro de y*. concluímos assim que* $1 + \sqrt{2}$ *é a unidade fundamental de* $Q(\sqrt{2})$*.*

Observação 2.2.1. *Notemos que uma solução para* $l^2 - 2m^2 = \pm 1$ *é* $(1, 1)$ *tal que* $\lambda = 1 + \sqrt{2}$ *é uma unidade.*

Exemplo 2.2.2. *O corpo* $\mathbb{Q}(\sqrt{2})$ *tem uma infinidade de unidades que são dadas por* $\pm\lambda^n$*, onde* $n = 0, \pm 1, \pm 2, \cdots$*. De fato, observe que* $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$*. Assim, se* ϵ *é uma unidade de* $\mathbb{Q}(\sqrt{2})$*, então* ϵ *é positiva ou negativa. Suponhamos, sem perda de generalidade, que* $\epsilon > 0$*. Uma vez que* $\lambda = 1 + \sqrt{2} > 1$ *podemos encontrar um inteiro* n *tal que* $\lambda^n \leq \epsilon < \lambda^{n+1}$*, e assim,* $\epsilon\lambda^{-n}$ *é uma unidade satisfazendo* $1 \leq \epsilon\lambda^{-n} < 1 + \sqrt{2}$*. Pelo Exemplo 2.2.1, segue que* $\epsilon\lambda^{-n} = 1$*, e deste modo,* $\epsilon = \lambda^n$*. Para o caso em que* $\epsilon < 0$ *o resultado segue de modo análogo.*

Exemplo 2.2.3. *A determinação da unidade fundamental pode ser feita da seguinte maneira:*

1. *Quando* $d \equiv 2 (mod\, 4)$ *ou* $d \equiv 3 (mod\, 4)$*. Se* $u = a + b\sqrt{d}$ *é uma unidade, com* $u \neq \pm 1$*, então* $-u, u^{-1}, -u^{-1}$ *são também unidades e somente um desses números é maior do que* 1*, uma vez que estes são exatamente os números* $\pm a \pm b\sqrt{d}$*. Assim,* $a + b\sqrt{d} > 1$ *somente quando* $a, b > 0$*, se* $u_1 = a_1 + b_1\sqrt{d}$ *é a unidade fundamental. Se* $u_m = u_1^m = a_m + b_m\sqrt{d}$*, então*

$$\begin{aligned} u_{m+1} &= u_1^{m+1} \\ &= a_{m+1} + b_{m+1}\sqrt{d} \\ &= u_1^m u_1 = (a_m + b_m\sqrt{d})(a_1 + b_1\sqrt{d}) \\ &= (a_1 a_m + b_1 b_m) + (a_1 b_m + b_1 a_m)\sqrt{d}. \end{aligned}$$

Assim,

$$b_{m+1} = a_1 b_m + b_1 a_m,$$

e portanto, $b_1 < b_2 < b_3 \cdots$. *Como* $N(u_1) = a_1^2 - b_1^2 d = \pm 1$, *segue que* $b_1^2 d = a_1^2 \pm 1$. *Assim, se escrevermos a sequência* $d, 4d, 9d, 16d, 25d, \cdots$, *então* b_1 *é o menor inteiro tal que* $b_1 > 0$ *e* $b_1^2 d$ *é um quadrado mais ou menos* 1. *Considerando, por exemplo, o corpo de números* $\mathbb{Q}(\sqrt{3})$, *ou seja, quando* $d = 3$, *tem-se que* $b_1^2 3 = a_1^2 \pm 1$. *Fazendo* $b_1 = 1$, *segue que* $b_1^2 3 = 3 = 2^2 - 1$, *e portanto,* $a_1 = 2$. *Como* b_1 *é o menor inteiro positivo para o qual isto ocorre, segue que* $b_1 = 1$ *e* $a_1 = 2$, *e portanto,* $u_1 = 2 + \sqrt{3}$ *é a unidade fundamental de* $\mathbb{Q}(\sqrt{3})$.

2. *Quando* $d \equiv 1 (mod\, 4)$. *Com argumento similar, segue que* $u_1 = \frac{a_1 + b_1\sqrt{d}}{2}$ *com* a_1 *e* b_1 *inteiros positivos de mesma paridade. Assim, se* u_1 *é uma unidade fundamental, então*

$$N(u_1) = \frac{a_1^2 - b_1^2\sqrt{d}}{4} = \pm 1,$$

se, e somente se, $b_1^2 d = a_1^2 \pm 4$. *Devemos, então, encontrar o menor inteiro positivo* $b_1 > 0$ *tal que* $b_1^2 d$ *é um quadrado mais ou menos* 4. *Consideramos, por exemplo, o corpo* $\mathbb{Q}(\sqrt{5})$, *isto é, quando* $d = 5$. *Assim,* $b_1^2 d = a_1^2 \pm 4$, *e fazendo,* $b_1 = 1$ *tem-se que* $b_1^2 5 = 5 = 3^2 - 4$, *ou seja,* $a_1 = 1$ *(uma vez que* $a_1 = 3$ *não convém). Como* $b_1 = 1$ *é o menor inteiro para o qual isto ocorre, segue que* $1 + \sqrt{5}$ *é a unidade fundamental de* $\mathbb{Q}(\sqrt{5})$.

2.3 Unidades em corpos ciclotômicos

O objetivo desta seção é apresentar o grupo das unidades de um corpo ciclotômico $\mathbb{K} = \mathbb{Q}(\xi_p)$, onde p é um número primo. Apresentamos as raízes das unidades de $\mathbb{K} = \mathbb{Q}(\xi_p)$ e veremos que toda unidade de $\mathcal{O}_\mathbb{K}$ pode ser escrita como o produto de uma unidade real por uma potência de uma raiz da unidade. As principais referências desta seção são [1] e [2].

Seja $\mathbb{K} = \mathbb{Q}(\xi)$, onde ξ é uma raiz p-ésima primitiva da unidade e p um primo ímpar. O polinômio minimal de ξ sobre $\mathbb{Q}(\xi)$ é dado por

$$\phi_p = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Portanto, ξ pertence ao anel de inteiros de $\mathbb{Q}(\xi)$ e as raízes de ϕ_p são dadas por $\xi, \xi^2, \xi^3, \cdots, \xi^{p-1}$. Assim,

$$\phi_p = \prod_{i=1}^{p-1}(x - \xi^i),$$

e deste modo,

$$\phi(1) = 1^{p-1} + 1^{p-2} + \cdots + 1^1 + 1 = \prod_{i=1}^{p-1}(1 - \xi^i) = p,$$

ou seja,

$$p = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}).$$

Lema 2.3.1. *Se p é um primo ímpar e $\xi = \xi_p$, então $p = u(1-\xi)^{p-1}$, onde u é uma unidade de $\mathbb{Z}[\xi]$.*

Demonstração: O primo p pode ser escrito como

$$p = (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}).$$

Se $1 \leq i, j \leq p-1$ e $k \in \mathbb{Z}$ são tais que $j \equiv ik (mod\, p)$ então

$$\frac{1-\xi^j}{1-\xi^i} = \frac{1-\xi^{ik}}{1-\xi^i} = \xi^{(k-1)i} + \cdots + \xi^{2i} + \xi^i + 1 \in \mathbb{Z}[\xi].$$

Analogamente,

$$\frac{1-\xi^i}{1-\xi^j} \in \mathbb{Z}[\xi].$$

Além disso,

$$\left(\frac{1-\xi^j}{1-\xi^i}\right) \cdot \left(\frac{1-\xi^i}{1-\xi^j}\right) = 1.$$

Assim, $\left\{\frac{1-\xi^i}{1-\xi^j}, \frac{1-\xi^j}{1-\xi^i}\right\}$ são unidades de $\mathbb{Z}[\xi]$, tomando se $u_i = \frac{1-\xi^i}{1-\xi} \in \mathbb{Z}[\xi]$, tem-se que $1 - \xi^i = u_i(1-\xi)$, onde u_i é uma unidade de $\mathbb{Z}[\xi]$ para $i = 1, 2, \cdots p-1$. Portanto,

$$\begin{aligned} p &= (1-\xi)(1-\xi^2)\cdots(1-\xi^{p-1}) \\ &= u_1(1-\xi)u_2(1-\xi)\cdots u_{p-1}(1-\xi) \\ &= u(1-\xi)^{p-1}, \end{aligned}$$

onde $u = u_1 u_2 \cdots u_{p-1}$ é uma unidade de $\mathbb{Z}[\xi]$. $\square$

Sejam p um primo ímpar, ξ uma raiz p-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\xi)$. Pelo Capítulo 1, segue que $[\mathbb{K} : \mathbb{Q}] = p - 1$ e o anel de inteiros de $\mathbb{K}$ é $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\xi]$.

Teorema 2.3.1. *O grupo multiplicativo W das raízes da unidade de $\mathbb{Q}(\xi)$ é dado por*

$$W = \{1, \xi, \xi^2, \cdots, \xi^{p-1}, -1, -\xi, -\xi^2, \cdots, -\xi^{p-1}\}.$$

Assim $o(W) = \omega = 2p$ e toda unidade de $u \in \mathbb{Q}(\xi)$ pode ser escrita na forma $u = \pm\xi^k v$, onde v é uma unidade real positiva de $\mathcal{O}_{\mathbb{K}}$.

Demonstração: O grupo W é um grupo multiplicativo cíclico de ordem finita, digamos igual a ω, como $-\xi \in W$ e $-\xi$ tem ordem $2p$, segue que $2p$ divide ω. Seja $x \in W$ 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,

$$\varphi(w) = \varphi(o(x)) = [\mathbb{Q}(x) : \mathbb{Q}] \text{ divide } p - 1 = [\mathbb{Q}(\xi) : \mathbb{Q}].$$

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 $mdc(p^r, m) = 1$, 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 $-1, -\xi, -\xi^2, \cdots - \xi^{p-1}, 1, \xi, \xi^2, \cdots, \xi^{p-1}$, são raízes da unidade distintas, segue que

$$W = \{-1, -\xi, -\xi^2, \cdots - \xi^{p-1}, 1, \xi, \xi^2, \cdots, \xi^{p-1}\}.$$

Agora, seja u uma unidade de $\mathbb{K} = \mathbb{Q}(\xi)$, como $\{1, \xi, \xi^2, \cdots, \xi^{p-2}\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}[\xi]$, segue que podemos escrever $u = a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{p-2}\xi^{p-2}$, onde $a_i \in \mathbb{Z}$ para $i = 1, 2 \cdots, p-2$. O conjugado complexo de u é também uma unidade e é dado por

$$\overline{u} = a_0 + a_1\xi^{-1} + a_2\xi^{-2} + \cdots + a_{p-2}\xi^{-(p-2)}.$$

Logo, $u' = u\overline{u}$ é também uma unidade, e além disso, se $u^{(k)} = a_0 + a_1\xi^k + a_2\xi^{2k} + \cdots + a_{p-2}\xi^{k(p-2)}$, onde $k = 1, 2, \cdots, p-1$, são os conjugados de u, então os conjugados de $\overline{u}$ são

$$\begin{aligned}\overline{u}^{(k)} = \sigma_k(\overline{u}) &= a_0 + a_1\xi^{-k} + \cdots + a_{p-2}\xi^{-k(p-2)} \\ &= a_0 + a_1(\overline{\xi^k}) + \cdots + a_{p-2}(\overline{\xi^{k(p-2)}}) \\ &= \overline{u^k}.\end{aligned}$$

Assim, os conjugados de u' são dados por $(u')^{(k)} = \sigma_k(u') = \sigma_k(u\overline{u}^{-1}) = \sigma_k(u)\sigma_k(\overline{u}^{-1}) = u^{(k)}[\overline{u}^{(k)}]^{-1} = u^{(k)}\overline{u^{(k)^{-1}}}$, Logo:

$$|\ (u')^{(k)}\ | = |\ u^{(k)}\overline{u^{(k)^{-1}}}\ | = |\ u^{(k)}u^{(k)^{-1}}\ | = |\ u^{(k)}u^{(k)^{-1}}\ | = |1| = 1,$$

com $k = 1, 2, \cdots, p-1$. Pela Proposição 2.1.3, segue que u' é uma raiz da unidade, e portanto, devemos ter $u' = \pm\xi^h$, com $0 \leq h \leq p-1$, afirmamos que $u' = \xi^h$. De fato, suponhamos que $u' = -\xi^h$ e consideremos o homomorfismo canônico

$$\begin{aligned}\theta : \mathbb{Z}[\xi] &\longrightarrow \tfrac{\mathbb{Z}[\xi]}{(1-\xi)\mathbb{Z}[\xi]} \\ x &\longmapsto \theta(x) = x + (1-\xi)\mathbb{Z}[\xi] = [x],\end{aligned}$$

onde $[x]$ representa a classe de equivalência de x em $\frac{\mathbb{Z}[\xi]}{(1-\xi)\mathbb{Z}[\xi]}$. Agora, como $1 - \xi \in (1-\xi)\mathbb{Z}[\xi]$, segue que $[1-\xi] = 0$ em $\frac{\mathbb{Z}[\xi]}{(1-\xi)\mathbb{Z}[\xi]}$, assim, $\theta(\xi) = [\xi] = [1] = 1$, e deste modo, $\theta(\xi^k) = \theta(\xi)^k = 1$, para $k = 1, 2, \cdots, p-2$. Além disso,

$$\begin{aligned}\theta(u) &= \theta(a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{p-2}\xi^{p-2}) \\ &= a_0 + a_1\theta(\xi) + a_2\theta(\xi)^2 + \cdots + a_{p-2}\theta(\xi^{p-2}) \\ &= a_0 + a_1 + a_2 + \cdots + a_{p-2} = \theta(\overline{u}).\end{aligned}$$

Como $u = -\xi^h\overline{u}$, segue que $\theta(u) = \theta(-\xi^h\overline{u}) = -\theta(\overline{u})$, assim, tem-se que $\theta(\overline{u}) = -\theta(\overline{u})$, ou seja, $\theta(2\overline{u}) = 0$, e portanto $2\overline{u} \in (1-\xi)\mathbb{Z}[\xi]$. Deste modo, existe $w \in \mathbb{Z}[\xi]$ tal que $2\overline{u} = (1-\xi)w$, e assim, $2 = (1-\xi)w\overline{u^{-1}}$, logo $1-\xi$ divide 2 em $\mathbb{Z}[\xi]$, o que implica que $(1-\xi)^{p-1}$ divide 2^{p-1}. Pelo Lema 2.3.1, segue que $p = w'(1-\xi)^{p-1}$, onde w' é uma unidade, e assim $(w')^{-1}p = (1-\xi)^{p-1}$, e deste modo, $p \mid (1-\xi)^{p-1}$ em $\mathbb{Z}[\xi]$. Logo,

$$(1-\xi)^{p-1} \mid 2^{p-1} \quad \text{e} \quad p \mid (1-\xi)^{p-1},$$

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 $u' = \xi^h$, e assim, $u = \xi^h \overline{u}$. Agora, seja k tal que $2k \equiv h(mod\, p)$. Assim, $\xi^h = \xi^{2k}$, e portanto:

$$\frac{u}{\xi^k} = \frac{\xi^h \overline{u}}{\xi^k} = \frac{\xi^k \xi^k \overline{u}}{\xi^k} = \xi^k \overline{u} = \frac{\overline{u}}{\xi^{-k}} = \overline{\left(\frac{u}{\xi^k}\right)} \in \mathbb{R}.$$

Seja $v = \frac{u}{\xi^k} = u\xi^{-k} = u\xi^{p-k} \in \mathbb{Z}[\xi]$. Como u e ξ^k são unidades segue que v é uma unidade real, e além disso,

$$u = \xi^k \left(\frac{u}{\xi^k}\right) = \xi^k v.$$

Agora, se $v > 0$ então $u = \xi^k v$, e se $v < 0$, então $v' = -v > 0$, ou seja, $u = -\xi^k(-v) = -\xi^k v'$, com $v' > 0$. Portanto, $u = \pm\xi^k v$, onde v é uma unidade real positiva. □

2.4 Teorema de Dirichlet

Nesta seção, estabelecemos alguns resultados necessários para a demonstração do Teorema das unidades de Dirichlet, que dará informações importantes a respeito da estrutura do grupo das unidades de um corpo abeliano $\mathbb{K}$, e definimos o regulador de $\mathbb{K}$ que será largamente explorado no capítulo 3. As principais referências desta seção são [1], [2] e [5].

Dado um corpo de números $\mathbb{K}$ de grau n sobre $\mathbb{Q}$, existem n imersões de $\mathbb{K}$ no corpo dos complexos $\mathbb{C}$. Destas n imersões tem-se que $r_1 \geq 0$ são reais e $2r_2 \geq 0$ são complexas, uma vez que os conjugados complexos aparecem aos pares, e assim, $n = r_1 + 2r_2$. Usamos as notações $\mathbb{K}^{(1)}, \mathbb{K}^{(2)}, \cdots, \mathbb{K}^{(n)}$ para os conjugados de $\mathbb{K}$, isto é, $\mathbb{K}^{(i)} = \sigma_i(\mathbb{K})$. Além disso, convencionamos que $\mathbb{K}^{(1)}, \mathbb{K}^{(2)}, \cdots, \mathbb{K}^{(r_1)}$ são os conjugados reais de $\mathbb{K}$ e que $\mathbb{K}^{(r_1+1)}, \cdots, \mathbb{K}^{(n)}$ são os corpos conjugados de $\mathbb{K}$ não reais. Deste modo, tem-se que $\overline{\mathbb{K}^{(r_1+j)}} = \mathbb{K}^{(r_1+r_2+j)}$, para $j = 1, 2, \cdots, r_2$. Se $x \in \mathbb{K}$, então $x^{(i)} \in \mathbb{K}^{(i)}$ é o conjugado de x, e assim, $\overline{x^{(r_1+j)}} = x^{(r_1+r_2+j)}$, para $j = 1, 2, \cdots r_2$.

Consideramos, agora, a seguinte aplicação

$$\begin{aligned} \lambda : U &\longrightarrow \mathbb{R}^r \\ u &\longmapsto \lambda(u) = (\log \mid u^{(1)} \mid, \log \mid u^{(2)} \mid, \cdots, \log \mid u^{(r)} \mid), \end{aligned}$$

onde $r = r_1 + r_2 - 1$, e $\mid u^{(i)} \mid$ denota o número real positivo que é o valor absoluto de $u^{(i)} \in \mathbb{C}$ e "log"o logaritmo natural.

Proposição 2.4.1. *Seja u uma unidade. Assim, u é uma raiz da unidade se, e somente se, $\lambda(u) = (0, 0, \cdots, 0) \in \mathbb{R}^r$.*

Demonstração: Se u é uma raíz da unidade, então pela Proposição 2.1.3, segue que $\mid u^{(j)} \mid = 1$, para todo conjugado de u. Assim, $\log(\mid u^{(j)} \mid) = \log(\mid 1 \mid) = 0$, para todo $j = 1, 2, \cdots, r, \cdots, n$, e portanto, $\lambda(u) = (0, 0, \cdots, 0)$. Reciprocamente, se $u \in U$ é tal que $\lambda(u) = (0, 0, \cdots, 0)$, o que equivale a $\mid u^{(1)} \mid = \mid u^{(2)} \mid = \cdots = \mid u^{(r)} \mid = 1$, então

$$\mid \mathrm{N}(u) \mid = \mid u^{(1)}u^{(2)} \cdots u^{(n)} \mid = 1.$$

Assim,

$$\log(1) = \log(\mid \mathrm{N}(u) \mid) = \log(\mid u^{(1)}u^{(2)} \cdots u^{(n)} \mid) = \sum_{i=1}^{n} \mid \log u^{(i)} \mid = 0.$$

Agora, como $\overline{x^{(r_1+j)}} = x^{(r_1+r_2+j)}$, segue em valores absolutos que $\mid x^{(r_1+j)} \mid = \mid x^{(r_1+r_2+j)} \mid$, para $j = 1, \cdots, r_2$, Assim, para $j = 1, \cdots, r_2 - 1$, segue que $2\log(\mid u^{(r_1+r_2)} \mid) = 0$, e portanto, $\mid u^{(r_1+r_2)} \mid = \mid u^{(r_1+2r_2)} \mid = \mid u^{(n)} \mid) = 1$, ou seja, $\mid u^{(i)} \mid = 1$, para todo $i = 1, 2, \cdots, n$. Pela Proposição 2.1.3, segue que u é uma unidade. □

Sejam $1 \leq q \leq r$ e $u_1, u_2, \cdots, u_q \in U$ tal que $\{\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_q)\} \subset \mathbb{R}^q$ é um subconjunto linearmente independente em $\mathbb{R}^r$. Seja

$$G = \left\{ (a_1, a_2, \cdots, a_q) \in \mathbb{R}^q;\ \text{existe}\ \ v \in U;\ \lambda(v) = \sum_{j=1}^{q} a_j \lambda(u_j) \right\}.$$

Propriedade 2.4.1. *Tem-se que $\mathbb{Z}^q \subset G$.*

Demonstração: Se $(a_1, a_2, \cdots, a_q) \in \mathbb{Z}^q$, então tomando-se $v = \prod_{i=1}^{q} u_j^{a_j}$, tem-se que $\lambda(v) = \lambda(\prod_{j=1}^{q} u_j^{a_j})$. Analisando coordenada a coordenada, segue que

$$\log \left| \prod_{j=1}^{q} u_j^{a_j} \right| = \sum_{j=1}^{q} a_j \log \mid u_j \mid,$$

e assim, $\lambda(v) = \sum_{j=1}^{q} a_j \lambda(u_j)$. Portanto, $(a_1, a_2, \cdots, a_q) \in G$, e deste modo, $\mathbb{Z}^q \subset G$. $\square$

Propriedade 2.4.2. *O conjunto G é um subgrupo aditivo de $\mathbb{R}^q$.*

Demonstração: Se $a = (a_1, a_2, \cdots, a_q)$ e $b = (b_1, b_2, \cdots, b_q)$ são elementos de G, então existem $v_1, v_2 \in U$ tal que

$$\lambda(v_1) = \sum_{j=1}^{q} a_j \lambda(u_j) \text{ e } \lambda(v_2) = \sum_{j=1}^{q} b_j \lambda(u_j).$$

Assim, se $v_1, v_2 \in U$, então $\frac{v_1}{v_2} \in U$, além disso,

$$\lambda\left(\frac{v_1}{v_2}\right) = \sum_{j=1}^{q} (a_j - b_j)\lambda(u_j).$$

Portanto, $a - b \in G$, e assim, G é um subgrupo de $\mathbb{R}^q$. $\square$

Seja $G_1 = \{(a_1, a_2, \cdots, a_q) \in G;\ 0 \leq a_i \leq 1 \text{ para todo } i = 1, 2, \cdots, q\}$.

Propriedade 2.4.3. *Toda classe de G relativa ao subgrupo $\mathbb{Z}^q$, contém um único elemento do subconjunto G_1, mais ainda, diferentes elementos em G_1 tem diferentes classes em $\frac{G}{\mathbb{Z}^q}$.*

Demonstração: Para a existência, se $(a_1, a_2, \cdots, a_q) + \mathbb{Z}^q \in \frac{G}{\mathbb{Z}^q}$, então $(a_1, a_2, \cdots, a_q) \in \mathbb{R}^q$. Agora, como todo número real se encontra entre dois números inteiros consecutivos, segue que podemos escrever

$$(a_1, a_2, \cdots, a_q) + \mathbb{Z}^q = (z_1, z_2, \cdots, z_q) + (x_1, x_2, \cdots, x_q) + \mathbb{Z}^q,$$

onde $(z_1, z_2, \cdots, z_q) \in \mathbb{Z}^q$ e $(x_1, x_2, \cdots, x_q) \in G_1$. Assim, segue que $(a_1, a_2, \cdots, a_q) + \mathbb{Z}^q = (x_1, x_2, \cdots, x_q) + \mathbb{Z}^q$, e deste modo, toda classe de $\mathbb{Z}^q$ contém elementos de G_1. Para a unicidade, suponhamos que uma classe de $\mathbb{Z}^q$ contenha pelo menos dois elementos $g, h \in G_1$. Assim, para todo $i = 1, 2, \cdots, q$, tem-se que $g = (g_1, g_2, \cdots, g_q)$, com $0 \leq g_i < 1$, e $h = (h_1, h_2, \cdots, h_q)$, com $0 \leq h_i < 1$. Deste modo, $\overline{g} = \overline{h} \Rightarrow \overline{g - h} = 0$, ou seja, $g_i - h_i \in \mathbb{Z}$. Logo, $g_i = h_i$, e portanto, $g = h$. $\square$

Lema 2.4.1. *O grupo* $\frac{G}{\mathbb{Z}^q}$ *é finito.*

Demonstração: Pela Propriedade 2.4.3, segue que é suficiente mostrar que G_1 é um conjunto finito. Para isto, seja $U_1 = \{v \in U : \text{existe}\,(a_1, a_2, \cdots, a_q) \in G_1 \,\text{tal que}\, \lambda(v) = \sum_{j=1}^{q} a_j\lambda(u_j)\}$. Se $v \in U_1$ e $(a_1, a_2, \cdots, a_q), (b_1, b_2, \cdots, b_q) \in G$ são tais que

$$\lambda(v) = \sum_{j=1}^{q} a_j\lambda(u_j) = \sum_{j=1}^{q} b_j\lambda(u_j),$$

então $\sum_{j=1}^{q}(a_j - b_j)\lambda(u_j) = 0$. Como, por hipótese, $\{\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_q)\}$ é um conjunto linearmente independente, segue que $(a_j - b_j) = 0$, e deste modo, $a_j = b_j$ para todo $j = 1, 2, \cdots, q$. Seja a aplicação

$$v \in U_1 \longmapsto (a_1, a_2, \cdots, a_q) \in G_1, \text{ onde } \lambda(v) = \sum_{j=1}^{q} a_j\lambda(u_j).$$

Pela definição de G_1, segue que a aplicação é sobrejetora. Assim, para mostrar que G_1 é finito, é suficiente mostrar que U_1 é um conjunto finito. Se $v \in U_1$, então

$$|\log(|\, v^{(i)}\,|)\,| = \left|\sum_{j=1}^{q} a_j log(|\, u_j^{(i)}\,|)\right| \leq \sum_{j=1}^{q} \log(|\, u_j^{(i)}\,|), i = 1, 2 \cdots, r.$$

Consideremos, agora, $\alpha_i = \sum_{j=1}^{q} log(|\, u_j^{(i)}\,| \geq 0$, para $i = 1, 2, \cdots, r$, e seja ainda, $\alpha = \max\{\alpha_1, \alpha_2, \cdots, \alpha_r\}$. Assim,

$$e^{-\alpha_i} \leq |\, v^{(i)}\,| \leq e^{\alpha_i} \leq e^{\alpha},$$

para $i = 1, 2, \cdots, r$.

Logo, existe $\beta > 0$ tal que $|\, v^{(i)}\,| \leq \beta$, para $i = 1, 2, \cdots, r$, pela Proposição 2.1.2, segue que U_1 é um conjunto finito, onde conclui-se a demonstração. □

Definição 2.4.1. *As unidades* $u_1, u_2, \cdots, u_k$ *de* $\mathcal{O}_{\mathbb{K}}$ *são ditas independentes quando a relação*

$$u_1^{m_1} u_2^{m_2} \cdots u_k^{m_k} = 1,$$

com $m_i \in \mathbb{Z}$, *para* $i = 1, 2, \cdots, k$, *for possível somente quando* $m_1 = m_2 = \cdots = m_k = 0$.

Observação 2.4.1. *Cada unidade u_i pertencente a um conjunto independente de unidades não pode ser uma raiz da unidade, uma vez que se u_i for uma uma raiz da unidade em um conjunto $\{u_1, u_2, \cdots, u_k\}$ de unidades independentes, então existe $m_i \neq 0$ tal que $u_1^{m_1} = 1$. Assim, $u_1^0 u_2^0 \cdots u_i^{m_i} \cdots u_k^0 = 1$, onde nem todos os expoentes são nulos, o que contraria o fato das unidades $u_1, u_2, \cdots, u_k$, serem independentes.*

Lema 2.4.2. *Se $u_1, u_2, \cdots, u_k$ são unidades de $\mathcal{O}_{\mathbb{K}}$, então as seguintes afirmações são equivalentes:*

1) $u_1, u_2, \cdots, u_k$ são unidades independentes.

2) $\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_k)$ são linearmente independentes sobre $\mathbb{Q}$.

3) $\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_k)$ são linearmente independentes sobre $\mathbb{R}$.

Demonstração: Para (1) implica (2), se $\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_k)$ são linearmente dependentes sobre $\mathbb{Q}$, então existem inteiros $\eta_1, \eta_2, \cdots, \eta_k$, não todos nulos, tal que $\sum_{j=1}^{k} \eta_j \lambda(u_j) = 0$. Assim, $\sum_{j=1}^{k} \eta_j \log(\mid u_j^{(i)} \mid) = 0$, para $i = 1, 2, \cdots, r$. Deste modo,

$$\begin{aligned} 0 &= \eta_1 \log(\mid u_1 \mid) + \eta_2 \log(\mid u_2 \mid) + \cdots + \eta_k \log(\mid u_k \mid) \\ &= \log(\mid u_1 \mid^{\eta_1}) + \log(\mid u_2 \mid^{\eta_2}) + \cdots \log(\mid u_k \mid^{\eta_k}) \\ &= \log(\mid u_1 \mid^{\eta_1} \mid u_2 \mid^{\eta_2} \cdots \mid u_k \mid^{\eta_k}) \\ &= \log(\mid u_1^{\eta_1} u_2^{\eta_2} \cdots u_k^{\eta_k} \mid) = 0, \end{aligned}$$

e assim, $\lambda(\prod_{j=1}^{k} u_j^{\eta_j}) = 0$. Pela Proposição 2.4.1, segue que $\prod_{j=1}^{k} u_j^{\eta_j}$ é uma raiz da unidade, ou seja, existe $h \geq 1$ tal que

$$(\prod_{j=1}^{k} u_j^{\eta_j})^h = 1.$$

Assim, $(\prod_{j=1}^{k} u_j)^{h\eta_j} = 1$, ou seja, $u_1^{h\eta_1} u_2^{h\eta_2} \cdots u_k^{h\eta_k} = 1$, com $h\eta_j$, para $j = 1, 2, \cdots, k$ não todos nulos, o que contradiz a hipótese de as unidades $u_1, u_2, \cdots, u_k$, serem independentes. Para (2) implica (3), se $\{\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_k)\}$ são linearmente dependentes

sobre $\mathbb{R}$, então por hipótese $\lambda(u_j) \neq (0, \cdots, 0) \in \mathbb{R}^r$, para todo $j = 1, 2, \cdots, k$. Após uma renumeração, caso necessário, pode-se assumir que $\{\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_q)\}$, com $0 < q \leq k$, é um conjunto linearmente independente sobre $\mathbb{R}$. Assim, cada $\lambda(u_s)$ tal que $q < s \leq k$, é da forma $\lambda(u_s) = a_j \sum_{j=1}^{q} \lambda(u_j)$, com $a_j \in \mathbb{R}$. Portanto, $(a_1, a_2, \cdots, a_q) \in G$. Se $h = \#(\frac{G}{\mathbb{Z}^q})$, então $ha_j \in \mathbb{Z}$, e assim, $a_j \in \mathbb{Q}$ para todo $j = 1, 2, \cdots, q$. Deste modo, $\{\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_k)\}$ é linearmente dependente sobre $\mathbb{Q}$, o que é uma contradição. Finalmente, para (3) implica (1), se $u_1, u_2, \cdots, u_k$ são dependentes em $\mathcal{O}_{\mathbb{K}}$, então existem inteiros $m_1, m_2, \cdots, m_k$ não todos nulos, tal que $u_1^{m_1} u_2^{m_2} \cdots u_k^{m_k} = 1$. Logo, $\sum_{j=1}^{k} m_j \lambda(u_j) = 0$, com $m_1, m_2, \cdots, m_k$ não todos nulos. Assim, $\{\lambda(u_1), \lambda(u_2), \cdots, \lambda(u_k)\}$ é linearmente dependente sobre $\mathbb{Z}$, e portanto, sobre $\mathbb{R}$, o que é uma contradição. □

Teorema 2.4.1 (Teorema de Minkowski). *Sejam $n > 1$ formas lineares dadas por $L_i = \sum_{i=1}^{n} a_{ij} X_i$, onde $i = 1, \cdots, n$, com coeficientes complexos tal que $d = \det(a_{ij}) \neq 0$. Assumimos que para todo i existe um índice i' tal que $\overline{L_{i'}} = \sum_{j=1}^{n} \overline{a_{ij}} X_j$ (o complexo conjugado da forma L_i) é igual a $L_{i'}$. Além disso, se L_i tem coeficientes reais, então $i = i'$. Se $\tau_1, \tau_2, \cdots, \tau_n$ são números reais positivos tal que $\overline{L_i} = L_{i'}$, então $\tau_i = \tau_{i'}$. Além disso, se $\tau_1 \tau_2 \cdots \tau_n \geq \mid d \mid$, dado algum índice i_0 tal que $\overline{L_{i_0}} = L_{i'_0}$, então existem inteiros $x_1, \cdots, x_n \in \mathbb{Z}$, não todos nulos, tal que $\mid L_i(x_1, \cdots, x_n) \mid < \tau_i$ para $i \neq i_0$ e $\mid L_i(x_1, \cdots, x_n) \mid \leq \tau_{i_0}$.*

Demonstração: Ver [1] cap 9, pag 157. □

Teorema 2.4.2 (Teorema de Dirichlet). *Sejam $\mathbb{K}$ um corpo de números de grau n, r_1 e r_2 os números definidos anteriormente e $r = r_1 + r_2 - 1$. O grupo U das unidades de $\mathbb{K}$ é isomorfo a $\mathbb{Z}^r \times W$, onde W é o grupo das raízes da unidade contidas em $\mathbb{K}$, isto é, $U \cong W \times \mathbb{Z}^r$.*

Demonstração: Primeiramente, mostramos que U é um grupo multiplicativo de tipo finito, e para isso calculamos seu rank. Consideramos a imersão canônica definida por

$(\sigma_1(x), \sigma_2(x), \cdots, \sigma_{r_1+r_2}(x))$ de $\mathbb{K}$ sobre $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, e a aplicação

$$\begin{array}{rcl} \lambda : \mathbb{K}^* & \longrightarrow & \mathbb{R}^{r_1+r_2} \\ x & \longrightarrow & \lambda(x) = (\log(\mid x^{(1)} \mid), \cdots, \log(\mid x^{(r_1+r_2)} \mid)). \end{array}$$

A aplicação λ é um homomorfismo (*chamado de imersão logarítmica de* $\mathbb{K}^*$). Seja B um subconjunto compacto de $\mathbb{R}^{r_1+r_2}$. Vamos mostrar que o conjunto B' das unidades de $x \in U$ tal que $\lambda(x) \in B$ é um conjunto finito. Como B é limitado, segue que existe um número real $\alpha > 1$ tal que para todo $x \in B'$, tem -se $\alpha^{-1} \leq \mid x^{(i)} \mid \leq \alpha$, pois as funções simétricas elementares são limitadas em valor absoluto. Uma vez que os coeficientes das funções simétricas estão em $\mathbb{Z}$ (já que $x \in \mathcal{O}_{\mathbb{K}}$), segue que o conjunto dos possíveis valores para uma função simétrica de $x^{(i)}$ é um conjunto finito. Portanto, existem finitas possibilidades de polinômios característicos para os elementos $x \in B'$, e consequentemente, existem somente finitos valores possíveis para x. Assim, B' é um conjunto finito, e a finitude de B' implica diretamente as seguintes propriedades:

1. O kernel da restrição de λ à U, é um grupo finito, e assim consiste das raízes da unidade. Como toda raiz da unidade de $\mathbb{K}$ pertence ao kernel de λ, segue que $ker(\lambda) = W$.

2. A imagem $\lambda(U)$ é um subgrupo discreto de $\mathbb{R}^{r_1+r_2}$, e consequentemente, $\lambda(U)$ é um $\mathbb{Z}$-módulo livre cujo rank é $s \leq r_1 + r_2$. Pelo primeiro teorema do isomorfismo, como $\lambda(U)$ é livre segue que U é isomorfo a $W \times \mathbb{Z}^s$.

Resta agora, mostrar que o rank s de $\lambda(U)$ é igual a r_1+r_2-1. A desigualdade $s \leq r_1+r_2-1$ segue do fato que se $x \in U$, então a relação

$$\pm 1 = \mathrm{N}(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_i(x)}$$

implica que o vetor $\lambda(x) = (y_1, \cdots, y_{r_1+r_2})$ pertence ao hiperplano H definido pela equação

$$\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1}^{r_1+r_2} y_j = 0.$$

Uma vez que $\lambda(U)$ é um subgrupo discreto de H, segue que

$$s \leq r_1 + r_2 - 1.$$

Para completar a demonstração necessitamos mostrar que existem $r = r_1 + r_2 - 1$ vetores independentes em $\lambda(U)$, isto é, que existem suficientes unidades independentes em U. Mas isto, é basicamente o conteúdo da seguinte afirmação: se $c_1, c_2, \cdots, c_r \in \mathbb{R}$, não todos nulos, então existe uma unidade $u \in U$ tal que

$$\sum_{i=1}^{r} c_i \log(\mid u^{(i)} \mid) \neq 0.$$

De fato, sejam $\{a_1, a_2, \cdots, a_n\}$ uma base integral de $\mathbb{K}$ e $d = \det(a_{ij})$, como d^2 é o discriminante do corpo $\mathbb{K}$, segue que $1 < d^2 \in \mathbb{Z}$, e assim, $1 <\mid d \mid$. Seja β um número real suficientemente grande, digamos

$$\beta \geq \left(\sum_{i=1}^{r} \mid c_i \mid \right) \log (\mid d \mid) + 1.$$

Consideramos as n formas lineares

$$L_i = \sum_{i=1}^{n} a_{ij} X_j, \;\; i = 1, \cdots, n.$$

Sejam $\tau_1, \tau_2, \cdots, \tau_n$ números reais positivos, satisfazendo as condições

1. $\tau_{r_1+i} = \tau_{r_1+r_2+i}$.
2. $\tau_1 \tau_2 \cdots \tau_n =\mid d \mid$.

Podemos escolher $\tau_1, \tau_2, \cdots, \tau_r$ arbitrariamente, e as relações acima determinam unicamente os demais. Pelo Teorema de Minkowski, segue que existem inteiros $x_1, \cdots, x_n$, não todos nulos, tal que se

$$y^{(i)} = L_i(x_1, x_2, \cdots, x_n) = \sum_{j=1}^{n} a_{ij} X_j,$$

então

$$\mid y^{(i)} \mid \leq \tau_i, \quad i = 1, \cdots, n.$$

Em particular, se $y \in \mathcal{O}_{\mathbb{K}}$, $y \neq 0$ e $1 \leq \mid \mathrm{N}(y) \mid \leq \mid d \mid$, então

$$\frac{\tau_i}{\mid d \mid} = \frac{\tau_i}{\tau_1 \tau_2 \cdots \tau_n} \leq \frac{1}{\prod\limits_{i \neq j} \mid y^{(i)} \mid} \leq \tau_i \leq \tau_i \mid d \mid .$$

Se

$$F(y) = \sum_{i=1}^{r} c_i \log(\mid y^{(i)} \mid),$$

então

$$\begin{aligned}
\left| F(y) - \sum_{i=1}^{r} c_i \log(\tau_i) \right| &= \left| \sum_{i=1}^{r} c_i \log(\mid y^{(i)} \mid) - \sum_{i=1}^{r} c_i \log(\tau_i) \right| \\
&= \left| \sum_{i=1}^{r} c_i \log \left(\frac{\mid y^{(i)} \mid}{\tau_i} \right) \right| \\
&\leq \sum_{i=1}^{r} \mid c_i \mid \left| \log \left(\frac{\mid y^{(i)} \mid}{\tau_i} \right) \right| \\
&\leq \left(\sum_{i=1}^{r} \mid c_i \mid \right) \log(\mid d \mid) < \beta,
\end{aligned}$$

uma vez que $-\log(\mid d \mid) \leq \log \underbrace{\left(\frac{\mid y^{(i)} \mid}{\tau_i} \right)}_{\leq 1} \leq 0 \leq \log(\mid d \mid)$. Suponhamos, agora, que para todo $h = 1, \cdots, r$ podemos escolher números reais positivos $\tau_{h1}, \tau_{h2}, \cdots, \tau_{hr}$ satisfazendo as condições do Teorema de Minkowski, e também, a seguinte condição adicional

$$\sum_{i=1}^{r} c_i \log(\tau_{hi}) = 2\beta h.$$

Isto é possível uma vez que existem índices i; $1 \leq i \leq r$, para o qual $c_i \neq 0$. Se $y_h \in \mathcal{O}_{\mathbb{K}}$, com $y_h \neq 0$, é obtido a partir de $\tau_{h1}, \tau_{h2}, \cdots, \tau_{hr}$, então

$$\mid F(y_h) - 2\beta h \mid = \left| F(y_h) - \sum_{i=1}^{r} c_i \log(\tau_{hi}) \right| \leq \beta,$$

e assim, $\mid F(y_h) - 2\beta h \mid \leq \beta$, logo $\beta(2h-1) < F(y_h) < \beta(2h-1)$, com $h = 1, \cdots, r$. Portanto,

$$F(y_1) < F(y_2) < F(y_3), \cdots$$

Mas,

$$\mathrm{N}(y_h\mathcal{O}_{\mathbb{K}}) \;=\; \mathrm{N}([y_h]) \;=\mid \mathrm{N}(y_h) \mid \leq \mid d \mid .$$

Assim, como $\mathrm{N}(y_h) \in \mathbb{Z}$ (pois $y_h \in \mathcal{O}_{\mathbb{K}}$), e como existe um número finito de ideais com a mesma norma, segue que existem índices $h \neq h'$ tal que $y_h\mathcal{O}_{\mathbb{K}} = \; y_{h'}\mathcal{O}_{\mathbb{K}}$. Portanto, $u = \frac{y_h}{y_{h'}}$ é uma unidade em $\mathbb{K}$, uma vez que F é linear. Assim,

$$F(y_h) \neq F(y_{h'}) = F(uy_h) = F(u) + F(y_h).$$

Logo, $F(u) \neq 0$, e assim

$$F(u) = \sum_{i=1}^{n} c_i \log(\mid u^{(i)} \mid) \neq 0,$$

o que completa a demonstração do teorema. □

Definição 2.4.2. *Todo conjunto de r unidades independentes $\{u_1, u_2, \cdots, u_r\}$ de $\mathbb{K}$, com $r = r_1 + r_2 - 1$, para os quais valem as propriedades do Teorema de Dirichlet é chamado um sistema fundamental de unidades em $\mathbb{K}$.*

Definição 2.4.3. *Seja $\{u_1, u_2, \cdots, u_r\}$ um sistema fundamental de unidades de $\mathbb{K}$. O número real positivo $R =\mid det(\log \mid u_j^{(i)} \mid) \mid$ é chamado o regulador de $\mathbb{K}$.*

Nosso interesse, agora, é mostrar que o regulador de $\mathbb{K}$ está bem definido, isto é, que independe do sistema de unidades escolhido, que é basicamente o conteúdo da seguinte proposição.

Proposição 2.4.2. *Se $\{u_1, u_2, \cdots, u_r\}$ e $\{v_1, v_2, \cdots, v_r\}$ são dois sistemas fundamentais de unidades de $\mathbb{K}$, então*

$$\mid det(\log \mid u_j^{(i)} \mid) \mid =\mid det(\log \mid v_j^{(i)} \mid) \mid .$$

Demonstração: Pelo Teorema de Dirichlet, podemos escrever

$$v_j = \xi^{b_j} u_1^{a_{1j}} u_2^{a_{2j}} \cdots u_r^{a_{rj}},$$

com $b_j, a_{ij} \in \mathbb{Z}$, para $j, i = 1, 2, \cdots, r$. Similarmente, podemos escrever

$$u_j = \xi^{b'_j} v_1^{a'_{1j}} v_2^{a'_{2j}} \cdots v_r^{a'_{rj}},$$

com $b'_j, a'_{ij} \in \mathbb{Z}$ para $j, i = 1, 2, \cdots, r$. Assim,

$$v_j = \xi^{b_j} u_1^{a_{1j}} u_2^{a_{2j}} \cdots u_{j-1}^{a_{r(j-1)}} \underbrace{\xi^{b'_j} v_1^{a'_{1j}} v_2^{a'_{2j}} \cdots v_r^{a'_{rj}}}_{u_j} \cdots u_r^{a_{rj}},$$

e portanto,

$$v_j = \xi^{b'_j + b_j a_{jj}} v_1^{a'_{1j}} v_2^{a'_{2j}} \cdots v_j^{a'_{ij} + a_{jj}} \cdots u_1^{a_{1j}} u_2^{a_{2j}} \cdots u_{j-1}^{a_{r(j-1)}} u_{j+1}^{a_{r(j+1)}} \cdots u_r^{a_{rj}}.$$

Pela unicidade da representação, segue que

$$a'_{ij} a_{ij} = \begin{cases} 1 & \text{se} \quad i = j \\ 0 & \text{se} \quad i \neq j. \end{cases}$$

Logo, $\left\| a'_{ij} \right\|$ é a matriz inversa da matriz $\|a_{ij}\|$, e assim,

$$\det(a_{ij}) \det(a'_{ij}) = 1.$$

Portanto,

$$|\det(a_{ij})| = |\det(a'_{ij})| = 1.$$

Agora, considerando os conjugados das unidades, seus valores absolutos e logaritmos, obtém-se que

$$|v_j^{(i)}| = |\xi^{b_j(i)} u_1^{a_{1j}(i)} u_2^{a_{2j}(i)} \cdots u_r^{a_{rj}(i)}| = |\xi^{b_j}| \, |u_1^{a_{1j}}| \, |u_2^{a_{2j}}| \cdots |u_r^{a_{rj}}|.$$

Aplicando o log segue que

$$\log(|v_j^{(i)}|) = \log(|\xi^{b_j}| \, |u_1^{a_{1j}}| \, |u_2^{a_{2j}}| \cdots |u_r^{a_{rj}}|) = \sum_{h=1}^{r} a_{hj} \log(|u_h^{(i)}|).$$

Assim,

$$\begin{aligned} \left| \det\left(\log(v_j^{(i)}) \right) \right| &= \left| \det\left(\sum_{h=1}^{r} a_{hj} \log(|u_h^{(i)}|) \right) \right| \\ &= \left| \det\left(\|a_{hj}\| \left\| \log |u_h^{(i)}| \right\| \right) \right| \\ &= \underbrace{|\det \|a_{hj}\||}_{=1} \left| \det \left\| \log |u_h^{(i)}| \right\| \right| \\ &= |\det(\log |u_h^{(i)}|)|, \end{aligned}$$

o que conclui a demonstração. □

2.5 Considerações finais do capítulo

Neste capítulo, apresentamos mais detalhadamente as unidades de um anel de inteiros, onde obtemos uma caracterização para essas unidades através da norma via a Proposição 2.1.5. Além disso, definimos as unidades fundamentais de um anel de inteiros que possibilitou definir o regulador R de um corpo $\mathbb{K}$, bem como demonstrar o Teorema das unidades de Dirichlet que é o principal resultado estabelecido neste capítulo.

Capítulo 3

Unidades especiais

Neste capítulo, tratamos as unidades de um corpo ciclotômico $\mathbb{Q}(\xi_n)$, no caso em que n é uma potência de primo, definimos o conceito de unidades ciclotômicas e por fim, introduzimos as unidades circulares. Na Seção (3.1), apresentamos alguns conceitos necessários para o desenvolvimento deste capítulo, exibimos o Teorema de Kroneck Weber e definimos o conceito de elemento ciclotômico. Por fim, trabalhamos com os Caracteres de Dirichlet que serão de grande importância no decorrer do capítulo. Na Seção (3.2), apresentamos o conceito de L-séries de Dirichlet e alguns de seus resultados básicos. Na Seção (3.3), tratamos das unidades ciclotômicas de $\mathbb{Q}(\xi_{p^m})$, onde p é um primo, e mostramos que o grupo das unidades ciclotômicas tem índice finito no grupo das unidades. Na Seção (3.4), definimos as unidades circulares segundo Thaine, as unidades circulares segundo Sinnott, e mostramos que em certas condições essas unidades coincidem.

3.1 Resultados básicos

O objetivo desta seção é introduzir algumas definições que consideramos básicas para o desenvolvimento deste capítulo, onde definimos os caracteres de Dirichlet e exibimos o Teorema de Kroneck-Weber. As principais referências desta seção são [1], [6] e [7].

Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o seu anel de inteiros. O anel $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind e assim todo ideal se fatora de modo único como o produto de ideais primos

de $\mathcal{O}_{\mathbb{K}}$. Se $\mathbb{L}$ é uma extensão finita de $\mathbb{K}$ e $\mathfrak{a}$ é um ideal de $\mathbb{K}$, então $\mathfrak{a}\mathcal{O}_{\mathbb{L}}$ é um ideal de $\mathcal{O}_{\mathbb{L}}$ gerado pelos elementos de $\mathfrak{a}$, e o ideal $\mathfrak{a}\mathcal{O}_{\mathbb{L}}$ é chamado de levantamento de $\mathfrak{a}$ em $\mathcal{O}_{\mathbb{L}}$.

Se $\mathfrak{p}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$, então existem inteiros e_i, com $i = 1, 2, \cdots, s$, tal que

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{i=1}^{s} \mathfrak{q}_i^{e_i},$$

onde os $\mathfrak{q}_i$ são os ideais primos $\mathfrak{q}$ de $\mathcal{O}_{\mathbb{L}}$ tal que $\mathfrak{q} \cap \mathcal{O}_{\mathbb{K}} = \mathfrak{p}$. Neste caso, dizemos que $\mathfrak{q}_i$ divide $\mathfrak{p}$, ou ainda, que $\mathfrak{q}_i$ é um ideal de $\mathbb{L}$ que está acima de $\mathfrak{p}$. Além disso, segue que

$$\sum_{i=1}^{s} e_i[\mathcal{O}_{\mathbb{L}}/\mathfrak{q}_i : \mathcal{O}_{\mathbb{K}}/\mathfrak{p}] = [\mathbb{L} : \mathbb{K}].$$

O número inteiro e_i é chamado índice de ramificação de $\mathfrak{q}_i$ na extensão $\mathbb{K} \subseteq \mathbb{L}$. Se ao menos um destes números for maior que 1, dizemos que o ideal primo $\mathfrak{p}$ se ramifica na extensão $\mathbb{K} \subseteq \mathbb{L}$. Se $e_i = 1$ para todo $i = 1, 2, \cdots, s$, dizemos que o ideal primo se decompõe completamente em $\mathbb{L}$. Se $e_i = [\mathbb{L} : \mathbb{K}]$, para algum i, então $s = 1$, e nesse caso, diz se que o ideal primo $\mathfrak{p}$ se ramifica completamente em $\mathbb{L}$.

Definição 3.1.1. *Sejam $\mathbb{K} \subseteq \mathbb{L}$ uma extensão galoisiana, $\mathfrak{p}$ um ideal primo de $\mathbb{K}$ que não se ramifica em $\mathbb{L}$ e $\mathfrak{p}'$ um ideal primo de $\mathbb{L}$ que está acima de $\mathfrak{p}$. Neste caso, existe um único $\mathbb{K}$-automorfismo γ de $\mathbb{L}$, que tem a seguinte propriedade*

$$\gamma(x) \equiv x^{|\mathcal{O}_{\mathbb{K}}/\mathfrak{p}|} (mod\ \mathfrak{p}'),$$

para todo $x \in \mathcal{O}_{\mathbb{L}}$. Esse $\mathbb{K}$-automorfismo é denominado automorfismo de Frobenius para o ideal primo $\mathfrak{p}'$ na extensão $\mathbb{K} \subseteq \mathbb{L}$.

Teorema 3.1.1 (Kronecker - Weber)**.** *Seja $\mathbb{K}$ um corpo de números. Se $\mathbb{K}$ é abeliano, então existe um número inteiro positivo n tal que $\mathbb{K} \subseteq \mathbb{Q}(\xi_n)$.*

Demonstração: Ver [6]. □

Definição 3.1.2. *Seja $\mathbb{K}$ um corpo abeliano. O menor inteiro positivo n tal que $\mathbb{K} \subseteq \mathbb{Q}(\xi_n)$ é chamado de condutor de $\mathbb{K}$.*

Definição 3.1.3. *Um elemento ciclotômico é um elemento do tipo*

$$\epsilon = \pm\xi_n^t \prod_{i=1}^{n-1}(1-\xi_n^j)^{b_i} \in \mathbb{Q}(\xi_n),$$

com n, t e b_i, números inteiros positivos com $i, j = 1, 2, \cdots, n-1$.

Um elemento ϵ é uma unidade ciclotômica quando ϵ e ϵ^{-1} pertencem a $\mathcal{O}_{\mathbb{K}}$. O conjunto de todas as unidades ciclotômicas forma um grupo que denotamos por C_n.

Definição 3.1.4. *Um caracter é um homomorfismo $\chi : G \longrightarrow \mathbb{C}^*$, onde G é um grupo abeliano finito.*

Dado um grupo abeliano finito G, seja $\widehat{G}$ o conjunto de todos os caracteres de G em $\mathbb{C}^*$. Em $\widehat{G}$ podemos definir o produto de dois caracteres de forma natural, isto é, se $\chi_1, \chi_2 \in \widehat{G}$, então $\chi_1\chi_2$ é a função de G em $\mathbb{C}^*$ definida por $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$, para todo $g \in G$.

No caso em que o grupo abeliano finito G é isomorfo a $(\mathbb{Z}/n\mathbb{Z})^*$, para algum número inteiro positivo n, dizemos que os caracteres de G são Caracteres de Dirichlet definidos *mod* n, ou simplesmente, um caracter *mod* n.

Se n divide m, então χ induz um homomorfismo de $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow \mathbb{C}^*$ pela composição natural com a aplicação $(\mathbb{Z}/m\mathbb{Z})^* \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. Portanto, podemos considerar χ definido *mod* m ou *mod* n. É conveniente considerar o caso quando n mínimo e chamamos n de condutor de χ, que denotamos por f_χ. Quando $\chi(a) = \chi(-a)$, dizemos que χ é um caracter par, e quando $\chi(a) = -\chi(a)$, dizemos que χ é um caracter ímpar.

3.2 L-séries

Nesta seção, apresentamos o conceito de L-Séries de Dirichlet e alguns resultados que por conveniência não serão demonstrados, mas serão usados no decorrer do capítulo. A principal referência desta seção é [6].

Definição 3.2.1. *Seja χ um caracter de Dirichlet definido mod f_χ. A L-série de Dirichlet definida por χ é dada por*

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

com $\Re(s) > 1$.

Definição 3.2.2. *Seja χ um caracter de Dirichlet definido mod f_χ. A soma Gaussiana é definida por*

$$\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a) e^{\frac{2\pi i a}{f_\chi}}.$$

O seguinte teorema será útil no decorrer da próxima seção, por uma questão de conveniência omitiremos sua demonstração.

Teorema 3.2.1. *Com as mesmas notações dadas anteriormente tem-se que*

$$L(1,\chi) = -\frac{\tau(\chi)}{f_\chi} \sum_{a=1}^{f_\chi} \overline{\chi}(a) \log \mid 1 - \xi_{f_\chi}^a \mid$$

se $\chi(-1) = 1$ e $\chi \neq 1$.

Demonstração: Ver [6]. □

Teorema 3.2.2. *Sejam $\mathbb{K}_m = \mathbb{Q}(\xi_n)$, onde $m > 2$, $m \not\equiv 2 (mod\, 4)$, e ξ_m uma raiz m-ésima primitiva da unidade. Sejam $\mathbb{K}_m^+ = \mathbb{K}_m \cap \mathbb{R}$, $h_m = h(\mathbb{K}_m)$ e $h_m^+ = h(\mathbb{K}_m^+)$ o número de classes de $\mathbb{K}_m$ e $\mathbb{K}_m^+$ respectivamente.*

Temos que

$$h_m^+ = \frac{1}{R^+} \prod_{\substack{\chi par \\ \chi \neq 1 \\ f_\chi \mid m}} \left(\frac{1}{2} \sum_{k=1}^{f_\chi} -\chi(k) \log \mid 1 - \xi_{f_\chi}^k \mid \right).$$

onde R^+ denota o regulador de $\mathbb{K}_m^+$.

Demonstração: ver [1] pag. 662 □

Lema 3.2.1. *Seja $\epsilon_1, \epsilon_2 \cdots, \epsilon_r$ unidades independentes de um corpo de números $\mathbb{K}$ gerando um subgrupo A de unidades de $\mathbb{K}$, e seja $\eta_1, \eta_2, \cdots, \eta_r$ gerando um subgrupo B; Se $A \subseteq B$ é de índice finito então*

$$[B : A] = \frac{R(\epsilon_1, \epsilon_2 \cdots, \epsilon_r)}{R(\eta_1, \eta_2, \cdots, \eta_r)}$$

Demonstração: ver [2] pag. 41 □

3.3 Unidades ciclotômicas

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. Nesta seção, estabelecemos esses resultados. A principal referência desta seção se encontra em [6].

Sejam $n \not\equiv 2(mod\, 4)$ e V_n o grupo multiplicativo gerado por

$$\{\pm\xi_n, 1 - \xi_n^a; 1 < a \leq n-1\}.$$

Sejam U_n o grupo das unidades de $\mathbb{Q}(\xi_n)$ e $C = V_n \cap U_n$. O grupo C é denominado de grupo das unidades ciclotômicas de $\mathbb{Q}(\xi_n)$. Mais geralmente, se $\mathbb{K}$ é um corpo de números abeliano, então podemos definir as unidades ciclotômicas de $\mathbb{K}$, tomando $\mathbb{K} \subseteq \mathbb{Q}(\xi_n)$ com n mínimo e definindo $C_{\mathbb{K}} = U_{\mathbb{K}} \cap C$, isto é, definimos as unidades ciclotômicas de um corpo abeliano $\mathbb{K}$ tomando se as unidades ciclotômicas do condutor deste corpo intersecção com as unidades do corpo $\mathbb{K}$.

A seguinte igualdade será útil ao longo desta seção. O elemento

$$\xi_n^{\frac{1-a}{2}} \left(\frac{1-\xi_n^a}{1-\xi_n}\right) = \pm\frac{sen\left(\frac{\pi a}{n}\right)}{sen\left(\frac{\pi}{n}\right)}$$

é real, e se substituirmos a por $-a$, então obtemos a mesma unidade multiplicada por -1.

No Capítulo 2, vimos as unidades ciclotômicas no caso em que n é primo, e agora, consideraremos o caso mais complicado, onde n é uma potência de primo.

Lema 3.3.1. *Seja p um primo e $m \geq 1$.*

1. *As unidades ciclotômicas de $\mathbb{Q}(\xi_{p^m})^+$ são geradas por -1 e as unidades*

$$\xi_a = \xi_{p^m}^{\frac{1-a}{2}} \left(\frac{1-\xi_{p^m}^a}{1-\xi_{p^m}} \right),$$

   com $1 < a < \frac{1}{2}p^m$ e $mdc(a,p) = 1$.

2. *As unidades ciclotômicas de $\mathbb{Q}(\xi_{p^m})$ são geradas por ξ_{p^m} e as unidades ciclotômicas de $\mathbb{Q}(\xi_{p^m})^+$.*

Demonstração: Para simplificar a notação, façamos $\xi = \xi_{p^m}$. A definição de unidades ciclotômicas envolve $1 - \xi^a$ para todo $a \not\equiv 0 (mod\, p^n)$. Se $k < m$ e $mdc(b,p) = 1$, então usando a relação

$$1 - X^{p^k} = \prod (1 - \xi^{p^{m-k}} X),$$

segue que

$$1 - \xi^{bp^k} = \prod_{j=0}^{p^k - 1} (1 - \xi^{b + jp^m - k}).$$

Uma vez que $mdc(p, b+jp^m-k) = 1$, podemos considerar somente os a com $mdc(a,p) = 1$. Como $1-\xi^a$ e $1-\xi^{-a}$ diferem por uma potencia de ξ, segue que é suficiente considerarmos $1 \leq a < \frac{1}{2}p^m$. Suponhamos, agora, que

$$\xi = \pm \xi^d \prod_{\substack{1<a<\frac{1}{2}p^m \\ mdc(a,p)=1}} (1-\xi^a)^{c_a}$$

é uma unidade de $\mathbb{Q}(\xi)$. Como os ideais $[1-\xi^a]$ são os mesmos (uma vez que $1-\xi^i$ e $1-\xi^j$ são associados para todo $i, j \in \mathbb{Z}$), segue que $\sum c_a = 0$. Portanto,

$$\zeta = \pm \xi^d \prod \left(\frac{1-\xi^a}{1-\xi} \right)^{c_a} = \pm \xi^e \prod_{a \neq 1} \xi_a,$$

onde $e = d \pm \frac{1}{2} \sum c_a (a-1)$. Note que, se $p = 2$ então $mdc(a,p) = 1$ se, e somente se, a for ímpar. Assim, ξ^e está em $\mathbb{Q}(\xi)$, e isto completa a prova do item (2). Se $\xi \in \mathbb{Q}(\xi)^+$, então cada fator do produto dado acima é real. Assim, $\pm\xi^e$ deve ser real, e portanto, deve ser igual a ± 1, o que conclui a demonstração. □

Lema 3.3.2. *Se G é um grupo abeliano finito e f é uma função de G com valores em um corpo de característica zero, então*

1. $\det(f(\sigma\tau^{-1}))_{\sigma,\tau\in G} = \prod_{\chi\in\widehat{G}} \sum_{\sigma\in G} \chi(\sigma)f(\sigma)$.
2. $\det(f(\sigma\tau^{-1}) - f(\sigma))_{\sigma,\tau\neq 1} = \prod_{\chi\neq 1} \sum_{\sigma\in G} \chi(\sigma)f(\sigma)$.
3. *Se* $\sum_{\sigma} f(\sigma) = 0$, *então* $\det(f(\sigma\tau^{-1}))_{\sigma,\tau\neq 1} = \mid G \mid^{-1} \prod_{\chi\neq 1} \sum_{\sigma\in G} \chi(\sigma)f(\sigma)$.

Demonstração: Ver [6], pg. 71. □

Mostramos, agora, que o grupo das unidades ciclotômicas é de índice finito no grupo de todas as unidades. Para isto, é suficiente considerarmos subcorpos reais. Começamos com o caso mais simples de se tratar, ou seja, quando n é potencia de primo.

Teorema 3.3.1. *Se p é um primo e $m \geq 1$, então as unidades ciclotômicas $C^+_{p^m}$ de $\mathbb{Q}(\xi_{p^m})^+$ é de índice finito no grupo das unidades $U^+_{p^m}$ e*

$$h^+_{p^m} = [U^+_{p^m} : C^+_{p^m}],$$

onde $h^+_{p^m}$ é o número de classes de $\mathbb{Q}(\xi_{p^m})^+$.

Demonstração: Mostramos que o regulador das unidades ξ_a do Lema 3.3.1 é não nulo. Para isto, sejam $\xi = \xi_p^m$ e a aplicação

$$\sigma_a : \xi \longmapsto \xi^a, \quad \sigma_a \in Gal(\mathbb{Q}(\xi) : \mathbb{Q}).$$

Sejam os elementos σ_a, para $1 \leq a < \frac{1}{2}p^m$ e $mdc(a,p) = 1$. Se $G = Gal(\mathbb{Q}(\xi)^+ : \mathbb{Q})$, então podemos escrever

$$\xi_a = \frac{\left(\xi^{\frac{-1}{2}}(1-\xi)\right)^{\sigma_a}}{\xi^{\frac{-1}{2}}(1-\xi)}.$$

Se $p = 2$, então estendemos σ_a para $\mathbb{Q}(\xi_{2^{m+1}})$, e tudo continua válido, uma vez que $\left|(\xi^{\frac{-1}{2}}(1-\xi))^{\sigma_a}\right|$ independe da escolha da extensão. Tomamos, agora, o elemento $f(\sigma) =$

$\log \mid \xi^{\frac{-1}{2}}(1-\xi)^{\sigma} \mid = \log \mid (1-\xi)^{\sigma} \mid$, com $\sigma \in G$. Aplicando o Lema 3.3.2, segue que

$$\begin{aligned}
R(\{\xi_a\}) &= \pm \det[\log \mid \xi_a^{\tau} \mid]_{a,\tau\neq 1} \\
&= \pm \det[f(\sigma\tau) - f(\tau)]_{\sigma,\tau\neq 1} \\
&= \pm \det[f(\tau\sigma^{-1} - f(\tau))]_{\sigma\tau\neq 1} \\
&= \pm \prod_{1\neq\chi\in\widehat{G}} \sum_{\sigma\in G} \chi(\sigma) f(\sigma) \\
&= \pm \prod_{1\neq\chi\in\widehat{G}} \sum_{\sigma\in G} \chi(\sigma) \log \mid (1-\xi)^{\sigma} \mid \\
&= \pm \prod \sum_{1\leq a\leq \frac{1}{2}p^m} \chi(a) \log \mid 1-\xi^a \mid \\
&= \pm \prod \frac{1}{2} \sum_{a=1}^{p^m} \chi(a) \log \mid 1-\xi^a \mid .
\end{aligned}$$

Se $f_\chi = p^k$, com $1 \leq k \leq m$, então usando a relação

$$\prod_{\substack{1<a<p^m \\ a\equiv b(mod\, p^k)}} (1-\xi_{p^m}^a) = 1 - \xi_{p^k}^b,$$

obtém-se que

$$\begin{aligned}
\sum_{a=1}^{p^m} \chi(a) \log \mid 1-\xi^a \mid &= \sum_{b=1}^{p^k} \chi(b) \log \mid 1-\xi_{p^k}^b \mid \\
&= \frac{f_\chi}{\tau(\overline{\chi})} L(1,\overline{\chi}) \\
&= -\tau(\chi) L(1,\overline{\chi}).
\end{aligned}$$

Logo,

$$R(\xi_a) = \pm \prod_{\chi\neq 1} -\frac{1}{2}\tau(\chi) L(1,\overline{\chi}) = h^+ R^+ \neq 0,$$

onde R^+ é o regulador de $\mathbb{Q}(\xi_{p^m})^+$. Portanto, $\pm\xi_a$ gera um subgrupo de índice finito no grupo de todas as unidades, a qual denotamos por C^+ e

$$[U_{p^m}^+ : C_{p^m}^+] = \frac{R(\xi_a)}{R^+} = h^+,$$

o que conclui a demonstração. □

Passamos, agora, ao caso mais geral, onde n é um inteiro qualquer. Neste caso, a demonstração é similar ao caso de potência de primos, mas neste caso devemos tomar alguns cuidados, uma vez que para isto necessitamos dos seguintes lemas.

Lema 3.3.3. *Se $f_\chi \nmid (\frac{n}{m})$, então*

$$\sum_{\substack{a=1 \\ mdc(a,n)=1}}^{n} \chi(a) \log \mid 1 - \xi_n^{am} \mid = 0.$$

Demonstração: Assumimos que existe $b \equiv 1 (mod\ (\frac{n}{m}))$ tal que $mdc(b,n) = 1$ e $\chi(b) \neq 1$, pois do contrário $\chi : \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*$ pode ser fatorado completamente em $\left(\frac{\mathbb{Z}}{\frac{n}{m}\mathbb{Z}}\right)^*$ e assim, $f_\chi \mid \frac{n}{m}$, o que é uma contradição. Como $\xi_n^{am} = \xi_n^{abm}$, segue que

$$\sum \chi(a) \log \mid 1 - \xi_n^{am} \mid = \sum \chi(a) \log \mid 1 - \xi_n^{abm} \mid = \chi(b)^{-1} \sum \chi(a) \log \mid 1 - \xi_n^{am} \mid .$$

Uma vez que $\chi(b) \neq 1$, segue que devemos ter o somatório nulo, ou seja, obtém-se que $\sum \chi(a) \log \mid 1 - \xi_n^{am} \mid = 0$, o que conclui a demonstração. □

Lema 3.3.4. *Seja $n = mm'$ com $mdc(m,m') = 1$. Se $f_\chi \mid m$, então*

$$\sum_{\substack{a=1 \\ mdc(a,n)=1}}^{n} \chi(a) \log \mid 1 - \xi_n^{am'} \mid = \phi(m') \sum_{\substack{b=1 \\ mdc(b,m)=1}}^{m} \chi(b) \log \mid 1 - \xi_m^{b} \mid .$$

Demonstração: Seja $a = b + cm$, com $1 \leq b < m$ e $0 \leq c < m'$. Se $mdc(a,n) = 1$, então $mdc(b,m) = 1$. Reciprocamente, para cada b com $mdc(b,m) = 1$, segue que existe $\phi(m')$ escolhas de c tal que $mdc(b + cm, m') = 1$. Portanto, $mdc(b + cm, n) = 1$, uma vez que $mdc(m,m') = 1$. Como $\chi(a)$ e $\xi_n^{am'}$ dependem somente de b, segue o resultado. □

Lema 3.3.5. *Se F, g, t são inteiros positivos com $f_\chi \mid F$ e $g \mid F$, então*

$$\sum_{\substack{a=1 \\ mdc(a,g)=1}}^{Ft} \chi(a) \log \mid 1 - \xi_{Ft}^{a} \mid = \sum_{\substack{b=1 \\ mdc(b,g)=1}}^{F} \chi(b) \log \mid 1 - \xi_F^{b} \mid .$$

Demonstração: Se $a = b + cF$, com $1 \leq b \leq F$ e $0 \leq c < t$, então $mdc(a, g) = 1$ se, e somente se, $mdc(b, g) = 1$. Além disso,

$$\prod_{c=0}^{t-1}(1 - \xi_{Ft}^{b+cF}) = 1 - \xi_F^b.$$

Uma vez que $\chi(a)$ depende somente de b, o resultado segue. □

Lema 3.3.6. *Se $f_\chi \mid m$, então*

$$\sum_{\substack{b=1 \\ mdc(b,m)=1}}^{m} \chi(b) \log \mid 1 - \xi_m^b \mid = \left[\prod_{p \mid m}(1 - \chi(p))\right] \sum_{b=1}^{m} \chi(b) \log \mid 1 - \xi_m^b \mid .$$

Demonstração: Ver [6], pg. 148. □

Teorema 3.3.2. *Sejam $n \not\equiv 2 (mod\, 4)$ e $n = \prod_{i=1}^{s} p_i^{e_i}$ sua fatoração em primos. Seja I percorrendo todos os subconjuntos próprios de $\{1, 2, \cdots, s\}$ (isto é, I percorre os subconjuntos de $\{1, 2, \cdots, s\}$ exceto $\{1, 2, \cdots, s\}$). Seja $n_I = \prod_{i \in I} p_i^{e_i}$, para $1 < a < \frac{1}{2}n$ e $mdc(a, n) = 1$. Se*

$$\xi_a = \xi_n^{da} \prod_I \frac{1 - \xi_n^{an_I}}{1 - \xi_n^{n_I}},$$

onde $da = \frac{1}{2}(1 - a)\sum_I n_I$, então $\{\xi_a\}$ forma um conjunto de unidades independentes para $\mathbb{Q}(\xi_n)^+$, onde C_n' denota o grupo gerado por -1 e as ξ_a's, e U_n^+ denota o grupo das unidades de $\mathbb{Q}(\xi_n)^+$. Além disso,

$$[U_n^+ : {C_n'}^+] = h_n^+ \prod_{\chi \neq 1} \prod_{p_i \nmid f_\chi} \left(\phi\left({p_i}^{e_i}\right) + 1 - \chi(p_i)\right) \neq 0,$$

onde h_n^+ é a número de classes de $\mathbb{Q}(\xi_n)^+$ e χ percorre todos os caracteres pares não triviais de $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Demonstração: A demonstração é similar a do Teorema 3.3.1, no entanto é um pouco mais técnica. Como na prova do Teorema 3.3.1, segue que

$$R(\{\xi_a\}) = \pm \prod_{\chi \neq 1} \frac{1}{2} \sum_{\substack{a=1 \\ mdc(a,n)=1}}^{n} \chi(a) \sum_{I} \log \mid 1 - \xi_n^{an_I} \mid,$$

onde χ percorre todos os caracteres pares não triviais $mod\, n$. Se $m' = n_I$ para algum I, então $n = mm'$ com $mdc(m, m') = 1$. Se $f_\chi \mid m$, então

$$\begin{aligned}
\sum_{\substack{a=1 \\ mdc(a,n)=1}}^{n} \log \mid 1 - \xi_n^{am'} \mid &= \phi(m') \sum_{\substack{b=1 \\ mdc(b,m)=1}}^{m} \chi(b) \log \mid 1 - \xi_m^{b} \mid \\
&= \phi(m') \left[\prod_{p \mid m} (1 - \chi(p)) \right] \sum_{b=1}^{m} \chi(b) \log \mid 1 - \xi_m^{b} \mid \\
&= \phi(m') \left[\prod_{p \mid m} (1 - \chi(p)) \right] \sum_{a=1}^{f_\chi} \chi(a) \log \mid 1 - \xi_{f_\chi}^{a} \mid \\
&= -\phi(m') \frac{f_\chi}{\tau(\overline{\chi})} L(1, \overline{\chi}) \prod_{p \mid m} (1 - \chi(p)) \\
&= -\phi(m') \tau(\chi) L(1, \overline{\chi}) \prod_{p \mid m} (1 - \chi(p)).
\end{aligned}$$

Se $n = n_I n_I'$, então $n_I = m'$ e $n_I' = m$. Portanto,

$$\begin{aligned}
\sum_{\substack{a=1 \\ mdc(a,n)=1}}^{n} \chi(a) \sum_{I} \log \mid 1 - \xi_n^{an_I} \mid &= -\tau(\chi) L(1, \overline{\chi}) \sum_{\substack{I \\ f_\chi \mid n_I'}} \phi(n_I) \prod_{p \mid n_I} (1 - \chi(p)) \\
&= h_n^+ R_n^+ \left(\sum_{\substack{I \\ f_\chi \mid n_I'}} \phi(n_I) \prod_{p \mid n_I'} (1 - \chi(p)) \right),
\end{aligned}$$

onde h_n^+ e R_n^+ são o número de classes e o regulador de $\mathbb{Q}(\xi_n)^+$, respectivamente. Agora,

se $n = \prod_{i=1}^{s} p_i^{e_i}$, então

$$\sum_{\substack{I \\ f_\chi | n'_I}} \phi(n_I) \prod_{p|n'_I} (1 - \chi(p)) = \prod_{p \nmid f_\chi} \left(\phi(p_i^{e_i}) + 1 - \chi(p_i)\right).$$

Expandindo o lado esquerdo da equação, segue que

$$\sum_J \phi\left(\sum_{i \in J} p_i^{e_i}\right) \prod_{i \notin J} (1 - \chi(p)),$$

onde J percorre todos os subconjuntos de $\{i; p_i \notin f_\chi\}$. Se $p \mid f_\chi$, então $1 - \chi(p) = 1$. Portanto, aumentamos o conjunto $i \notin J$ para incluir todo $i \notin J$ com $1 \leq i \leq s$. Se $n_J = \prod_{i \in J} p_i^{e_i}$ e $n'_J = \prod_{i \notin J} p_i^{e_i}$, então

$$\sum_J \phi(n_J) \prod_{p|n'_J} (1 - \chi(p)),$$

uma vez que J esta incluso na soma se, e somente se, $mdc(n_J, f_\chi) = 1$ se, e somente se, $f_\chi \mid n'_J$. Assim, se $f_\chi \neq 1$, então $n_J \neq 1$, e deste modo, $J \neq \{1, 2, \cdots, s\}$ como requerido. Finalmente, como a parte real de $(\phi(p_i^{e_i}) + 1 - \chi(p_i))$ é positiva, segue que esse produto é não nulo. Como $[U_n^+ : C_n^+]$ é a razão dos reguladores $R(\{\xi_a\})/R_n^+$, segue o resultado. □

Corolário 3.3.1. *Se C'' é o grupo gerado por -1 e as unidades da forma*

$$\xi_n^{\frac{(1-a)}{2}} \left(\frac{1 - \xi_n^a}{1 - \xi_n}\right) \quad com \quad 1 < a < \frac{1}{2}n, \; mdc(a, n) = 1,$$

então

$$[U_n^+ : C''_n] = h_n^+ \prod_{\chi \neq 1} \prod_{p|n} (1 - \chi(p)),$$

onde χ percorre todos os caracteres pares não triviais definidos mod m, e o índice é infinito se, e somente se, o lado direito da equação for nulo.

Demonstração: Ver [6], pg 150. □

3.4 Unidades circulares

Em [7] Nobrega define o grupo das unidades circulares segundo Sinnott que denotamos por $C_S(\mathbb{K})$, e define, também, o grupo das unidades circulares segundo Thaine denotado por $C_S(\mathbb{K})$. Além disso, mostra que em certas condições esses dois grupos coincidem, e são estes resultados que estabelecemos nesta seção.

Sejam $\mathbb{K}$ um corpo abeliano de condutor m e $\mathbb{K}'_n$ a intersecção de $\mathbb{K}$ com $\mathbb{Q}(\xi_n)$, onde $n \in \mathbb{N}$. Seja, ainda, $\alpha(n,\, a)$ a norma de $\mathbb{Q}(\xi_n)$ sobre $\mathbb{K}'_n$ dos elementos $1-\xi_n^a$, com $n \in \mathbb{N},\ n>2$ e $a = 1, 2, \cdots, n-1$.

Definição 3.4.1. *O grupo das unidades circulares definido por Sinnott, denotado por $C_S(\mathbb{K})$, é definido como sendo a interseção de $\mathcal{O}_{\mathbb{K}}^*$ com o subgrupo de $\mathbb{K}^*$ gerado pelos elementos* $\{1, -1,\ \cdots,\ \alpha\,(n,\, a)\}\ \ , n \in \mathbb{N},\ n>2\ \ a = 1, \cdots, n-1$.

Definição 3.4.2. *O grupo das unidades circulares definido por Thaine, denotado por $C_T(\mathbb{K})$, é definido por*

$$C_T(\mathbb{K}) = \bigcup_{j=1}^{\infty} C_j(1),$$

onde

$$C_j(X) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{r=1}^{m-1} (X^i - \xi_m^r)^{a_{ir}},\ \textit{tal que}\ ,\ \ a_{ir} \in \mathbb{Z}, f(X) \in \mathbb{K}[X]\ \ \textit{e}\ f(1) \in \mathcal{O}_{\mathbb{K}}^* \right\},$$

m é o condutor de $\mathbb{K}$ e j é um número inteiro positivo.

Para cada número inteiro positivo n tal que $m \mid n$ e j é um inteiro positivo, seja

$$C_j(X,\, n) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{r=1}^{n-1} (X^i - \xi_n^r)^{a_{ir}},\ \text{tal que}\ ,\ \ a_{ir} \in \mathbb{Z}, f(X) \in \mathbb{K}[X]\ \ \text{e}\ f(1) \in \mathcal{O}_{\mathbb{K}}^* \right\}.$$

Seja, ainda,

$$C_j(1,\, n) = \{ f(1) :\ \ f(X) \in C_j(X,\, n) \}\,.$$

O conjunto $C_j(1,\, n)$ tem estrutura de grupo para qualquer n múltiplo de m e $j \in \mathbb{N}$. Além disso, $C_1(1,\, n) \subseteq C_2(1,\, n) \subseteq \cdots$, uma vez que se $f(X) \in C_j(X,\, n)$, então $f(X) =$

$\pm\prod_{i=1}^{j}\prod_{r=1}^{n-1}(X^i-\xi_n^r)^{a_{ir}}$. Assim, podemos considerar $f(X)=\pm\prod_{i=1}^{j+1}\prod_{r=1}^{n-1}(X^i-\xi_n^r)^{b_{ir}}$, onde $b_{ir}=\begin{cases} a_{ir}, & \text{se } i\leq j \\ 0, & \text{se } i=j+1. \end{cases}$

Assim, tem-se que $C_j(X,\,n)\subseteq C_{j+1}(X,\,n)$, e portanto, $C_j(1,\,n)\subseteq C_{j+1}(1,\,n)$. Deste modo, conclui-se que $\bigcup_{j=1}^{\infty}C_j(1,\,n)$ é um grupo, o qual denotamos por $C(n)$. Além disso, tem-se que $C(m)=C_T(\mathbb{K})$ (ver [7]).

Lema 3.4.1. *Seja $\mathbb{K}$ um corpo abeliano de condutor m. Se $j,n\in\mathbb{Z}^+$ e x é uma indeterminada, então*

1. *$C_j(x,\,n)\subseteq C_1(x,\,tn)$, para algum inteiro positivo t.*
2. *$C_1(1,\,n)\subseteq C_1(1,tn)$, para algum inteiro positivo t.*
3. *$C=\bigcup_{t=1}^{\infty}C_1(1,tm)$ é um grupo.*
4. *$C_T(\mathbb{K})\subseteq C$.*

Demonstração: Para o item (1), se $f(x)\in C_j(x,n)$, então as raízes de $f(x)$ são raízes dos polinômios $x^i-\xi_n^r$, com $i=1,2,\cdots,j$ e $r=1,2,\cdots,n-1$. Assim, se θ é uma raiz de $f(x)$, então $\theta^i=\xi_n^r$, e portanto, $\theta^{in}=\xi_n^{rn}=1$. Deste modo, as raízes de $f(x)$ são as raízes tn-ésimas da unidade, onde $t=1,2,\cdots,j$. Assim, $f(x)=\pm\prod_{i=1}^{(tn)-1}(x-\xi_{tn}^i)^{b_i}\in C_1(x,tn)$, e portanto, $C_j(x,n)\subseteq C_1(x,tn)$. Para (2), se $f(x)\in C_1(x,n)$, então $f(x)=\pm\prod_{i=1}^{n-1}(x-\xi_n^i)^{a_i}=\pm\prod_{i=1}^{(tn)-1}(x-\xi_{tn}^i)^{b_i}$, onde $b_i=\begin{cases} a_{i/t}, & \text{se } i\equiv 0(mod\ t) \\ 0, & \text{caso contrário,} \end{cases}$ e portanto, $f(x)\in C_1(x,tn)$, ou seja, $f(1)\in C_1(1,tn)$. Para (3), se $f(1),g(1)\in C$, então podemos supor, sem perda de generalidade, que $f(1)\in C_1(1,t_1m)$ e $f(1)\in C_1(1,t_2m)$ com t_1,t_2 inteiros positivos. Pelo item (2), segue que $C_1(1,t_1m),C_1(1,t_2m)\subseteq C_1(1,t_1t_2m)$. Agora, como $C_1(1,t_1t_2m)$ é um grupo, segue que $f(1)g(1)\in C_1(1,t_1t_2m)\subseteq C$. Para (4), vimos que $C_T(\mathbb{K})=C(m)=\bigcup_{j=1}^{\infty}C_j(1,m)$. Agora, pelo item (1), segue que $C_j(1,m)\subseteq C_1(1,tm)$

para algum inteiro positivo t, e portanto, $\bigcup_{j=1}^{\infty} C_j(1,m) \subseteq \bigcup_{t=1}^{\infty} C_1(1,tm) = C$, ou seja, $C_T(\mathbb{K}) \subseteq C$. □

Lema 3.4.2. *Se* $f(x) = \prod_{i=1}^{m-1}(x-\xi_m^i)^{a_i} \in \mathbb{K}[x]$, *então* $f(x) = \prod_{j|m} f_j(x)$, *onde* $f_j(x) = \prod_{\substack{i=1 \\ mdc(i,m)=j}}^{m-1}(x-\xi_m^i)^{a_i} \in \mathbb{K}'_{n/j}[x]$.

Demonstração: Ver [7]. □

Lema 3.4.3. *Sejam* n *um número inteiro positivo,* $\mathbb{L}$ *um subcorpo de* $\mathbb{Q}(\xi_n)$ *e* $G = Gal(\mathbb{Q}(\xi_n) : \mathbb{L})$. *Se* $\{\theta_1, \theta_1, \cdots, \theta_s\}$ *é um conjunto de representantes das classes de* G_n/G, *onde* $G_n = Gal(\mathbb{Q}(\xi_n) : \mathbb{K})$, *então*

1. *os polinômios* $g_i(x) = \prod_{\gamma \in G}(x - \xi_n^{\theta_i \gamma})$ *pertencem a* $\mathbb{L}[x]$ *e são irredutíveis em* $\mathbb{L}$, *onde* $i = 1, 2, \cdots, s$,

2. $g_i(1) = N_{\mathbb{Q}(\xi_n)/\mathbb{L}}(1 - \xi_n^{\theta_i \gamma})$, *onde* $i = 1, 2, \cdots, s$,

3. *o grupo multiplicativo*

$$S = \left\{ g(x) = \prod_{i=1}^{n-1}(x - \xi_n^i)^{a_i};\ a_i \in \mathbb{Z} \ \text{ e } g(x) \in \mathbb{L}[x] \right\}$$

é um $\mathbb{Z}$*-módulo livre de posto* $[\mathbb{L} : \mathbb{Q}]$ *e gerado por* $\{g_i(X) : \ para\, i = 1, 2, \cdots, s\}$.

Demonstração: Ver [7]. □

Com esses resultados já estabelecidos, chegamos ao ponto crucial desta seção, onde mostramos que as unidades circulares de Sinnott e as unidades circulares de Thaine coincidem.

Teorema 3.4.1. *Seja* $\mathbb{K}$ *um corpo abeliano de condutor* m. *Se* $C_T(\mathbb{K})$ *é o grupo das unidades circulares de Thaine e* $C_S(\mathbb{K})$ *é o grupo da unidades circulares de Sinnott, então*

$$C_T(\mathbb{K}) = C_S(\mathbb{K}).$$

Demonstração: Inicialmente, mostramos que $C_S(\mathbb{K}) \subseteq C_1(1)$. Para isto, se $\delta \in C_S(\mathbb{K})$, então $\delta = \prod_{n|m} \delta_n$, onde $\delta_n = \prod_{\alpha=1}^{n-1} \alpha(n,\, a)^{b_{n,a}}$. Sejam $f_{n,a}(x) = \prod_{\mu \in G} (X - \xi_n^{a\mu})$, onde $G = Gal(\mathbb{Q}(\xi_n) : \mathbb{K})$, $f_n(x) = \prod f_{n,a}^{b_{n,a}}(x)$ e $F(x) = \prod_{n|m} f_n(x)$. Observamos, agora, que $f_{n,a}(x) \in \mathbb{K}[x]$ e $f_{n,a}(1) = \alpha(n,a)$. Assim,

$$f_n(1) = \prod f_{n,a}(1) = \prod \alpha(n,a) = \delta_n$$

e

$$F(1) = \prod_{n|m} f_n(1) = \prod_{n|m} \delta_n = \delta.$$

Como $F(x) = \prod_{n|m} f_n(x)$, segue que podemos escrever $F(x) = \prod_{i=1}^{m-1} (x - \xi_m^i)^{a_i}$, com $F(x) \in \mathbb{K}[x]$, uma vez que $f_{n,a} \in \mathbb{K}[x]$ e $F(1) \in \mathcal{O}_{\mathbb{K}}^*$. Portanto, $\delta = F(1) \in C_1(1)$, e assim, $C_S(\mathbb{K}) \subseteq C_1(1)$. Mostramos, agora, que $C \subseteq C_S(\mathbb{K})$. Para isto, seja $\delta \in C$. Assim, $\delta \in C_1(1,\, n)$ para algum n múltiplo de m. Se $f(x) = \prod_{i=1}^{n-1} (x - \xi_n^i)^{a_i} \in \mathbb{K}[x]$ tal que $f(1) = \delta$, pelo Lema 3.4.2, segue que podemos escrever $f(x) = \prod_{j|n} f_j(x)$, com $f_j(x) \in \mathbb{K}'_{n/j}[x]$. Pelo Lema 3.4.3, segue que para cada divisor j de n existem polinômios $g_{ij}(x) \in \mathbb{K}'_{n/j}[x]$ tal que $f_j(x) = \prod_i g_{ij}^{b_{ij}}(x)$ e $g_{ij}(1) = \mathrm{N}_{\mathbb{Q}(\xi_{(n/j)})/\mathbb{K}'_n}(1 - \xi_{n/j}^i)$. Assim, aplicando $f_j(x)$ em 1 tem-se que $f_j(1) = \prod_i \mathrm{N}_{\mathbb{Q}(\xi_{(n/j)})/\mathbb{K}'n}(1 - \xi_{n/j}^i)^{b_{ij}}$, e portanto, $f(1) = \prod_{j|n} f_j(1) \in C_S(\mathbb{K})$. Já havíamos mostrado que $C_T(\mathbb{K}) \subseteq C$, e provamos agora que $C_T(\mathbb{K}) \subseteq C_S(\mathbb{K})$, visto que $C_T(\mathbb{K}) \supseteq C_1(1) \supseteq C_S(\mathbb{K})$. Portanto, concluímos que $C_T(\mathbb{K}) = C_S(\mathbb{K})$. □

3.5 Considerações finais do capítulo

Neste capítulo, apresentamos as unidades ciclotômicas e mostramos que o grupo das unidades ciclotômicas tem índice finito no grupo de todas as unidades. Definimos também duas classes especiais de unidades, as unidades circulares de Sinnott $C_S(\mathbb{K})$ e as unidades

circulares de Thaine $C_T(\mathbb{K})$, e mostramos que para um corpo abeliano $\mathbb{K}$ de condutor m, tais grupos de unidades coincidem.

Capítulo 4

Conclusões e perspectivas

Neste trabalho, tratamos as unidades dos anéis de inteiros de certos corpos abelianos. Para isso, inicialmente, tratamos alguns resultados da teoria dos números para obtermos a base teórica necessária para o desenvolver do trabalho. Apresentamos de forma genérica o conceito de elemento inteiro sobre um anel, e vimos que o conjunto dos inteiros sobre um anel tem estrutura de anel. Em seguida, nos dedicamos ao estudo dos elementos invertíveis deste anel, isto é, as unidades do anel de inteiros. Usando a norma de um elemento $x \in \mathbb{K}$ caracterizamos as unidades de $\mathcal{O}_{\mathbb{K}}$, como sendo os elementos inteiros que tem norma igual a 1. Demonstramos o Teorema das unidades de Dirichlet, que dá informações sobre a estrutura do grupo U das unidades de um corpo abeliano $\mathbb{K}$, onde usamos como base o Teorema de Minkowiski.

Explicitamos as unidades de corpos quadráticos $\mathbb{Q}\left(\sqrt{d}\right)$, com d um inteiro livre de quadrados, e de corpos ciclotômicos $\mathbb{Q}(\xi)$, onde ξ é uma raiz p-ésima primitiva da unidade e p um número primo. Nestes casos, por serem mais simples podemos dar o anel de inteiros bem como suas unidades de forma explicita. Apresentamos, também, a estrutura do grupo das unidades de $\mathbb{Q}(\xi_n)$, quando n é potência de um primo. Apoiados no Teorema de Kronecker-Weber definimos as unidades ciclotômicas de um corpo abeliano qualquer $\mathbb{K}$ como sendo a intersecção do grupo das unidades de $\mathbb{K}$ com o grupo das unidades do condutor de $\mathbb{K}$, e mostramos que o grupo das unidades ciclotômicas é de índice finito no grupo das unidades.

Como perspectiva de estudos futuros, podemos aplicar a teoria das unidades para a obtenção de códigos corretores mais eficazes.

A teoria de códigos corretores de erros surgiu com o matemático Claude A. Shanon, e consiste em codificar uma informação que é enviada de uma fonte através de um canal até um receptor. Ao enviar uma informação através de uma canal, a mesma pode sofrer interferências que chamamos de ruídos do canal. Um código corretor de erros é uma forma de detectar e corrigir erros que possam vir a ocorrer na transmissão. Separando as palavras códigos em esferas no espaço $\mathbb{R}^n$ com um raio d, chamado de distancia mínima, podemos associar um código corretor com um reticulado no $\mathbb{R}^n$, isto é, com um subconjunto discreto do $\mathbb{R}^n$. Tal interpretação nos leva ao problema do empacotamento esférico de Hilbert, que visa cobrir o espaço $\mathbb{R}^n$ com esferas de mesmo raio de modo a cobrir a maior área possível. Assim resolver o problema do empacotamento esférico equivale a encontrar códigos eficientes, o que motivou o estudo e a descoberta de várias classes de reticulados.

Minkowski mostrou que tomando-se um corpo de números $\mathbb{K}$ de grau n, o seu anel de inteiros $\mathcal{O}_{\mathbb{K}}$ e um homomorfismo chamado de homomorfismo de Minkowski de modo que a imagem de um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ seja um reticulado de posto n no $\mathbb{R}^n$. Tal reticulado é chamado de reticulado algébrico e a partir deste, pode se determinar reticulados com densidade ótima para diversas dimensões e assim códigos perfeitos. Como observamos, a teoria algébrica dos números se mostrou uma ferramenta muito eficaz para resolver problemas prático na área de telecomunicação.

Finalmente, observamos que muitas questões desta teoria ainda se encontram em aberto e muitos resultados particulares podem ser obtidos através de futuros estudos na descoberta de outras unidades, e também, em aplicações na teoria da informação e da codificação.

Referências Bibliográficas

[1] RIBENBOIM, P. Classical Theory of Algebraic Numbers. New York: Springer-Verlag, 2001.

[2] SAMUEL, P. Algebraic Theory of Numbers. Paris: Hermann, 1970.

[3] POLLARD, H.; DIAMOND. H. G. The Theory of Algebric Numbers. New York: Dover, 1998.

[4] STEWART, I. N.; TALL, D. O. Algebraic Number Theory and Fermat's Last Theorem. London: A K Peters, Ltd, 1945.

[5] ALACA, S.; WILLIAMS K. S. Introductory Algebric Number Theory. New York: Cambridge, 2004.

[6] WASHINGTON, L. C. Introduction to Cyclotomic Fields. New York: Springer-Verlag, 1982.

[7] NOBREGA, T. P. N. Unidades de Corpos Abelianos. Campinas: UNICAMP, 1991. 1-68 p. Tese (Doutorado) - Programa de Pós-Graduacão em Matemática, Universidade Estadual de Campinas, Campinas, 1991.

[8] LANG, S. Algebraic Number Theory. New York: Springer-Verlag, 1994.

[9] LANG, S. Cyclotomic Fields I and II. New York: Springer-Verlag, 1990.

[10] ATIYAH, M. F.; MACDONALD, I. J. Introduction to Commutative Algebra. London: Addison-Wesley, 1969.

Autorizo a reprodução xerográfica para fins de pesquisa.

São José do Rio Preto, 08 / 03 / 2013

Assinatura