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

Tópicos de Teoria dos Números Algébricos e Aplicações em Reticulados e Equações Diofantinas

Paulo Roberto da Silva

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

Orientadora
Profa. Dra. Carina Alves

2015

512.7 Silva, Paulo Roberto da
S586t Tópicos de Teoria dos Números Algébricos e aplicações em reticulados e equações diofantinas / Paulo Roberto da Silva. - Rio Claro, 2015
79 f. : il., figs., tabs.

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

1. Teoria dos números. 2. Extensões de corpos. 3. Número de classe. 4. Ideais primos. 5. Base integral. 6. Unidades. I. Título.

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

TERMO DE APROVAÇÃO

Paulo Roberto da Silva

Tópicos de Teoria dos Números Algébricos e Aplicações em Reticulados e Equações Diofantinas

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

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Eliris Cristina Rizziolli
IGCE- UNESP (Rio Claro)

Profa. Dra. Grasiele Cristiane Jorge
UNIFESP (São José dos Campos)

Rio Claro, 17 de setembro de 2015

Agradecimentos

Para que esta dissertação fosse escrita, foram necessários meses de dedicação e estudo, e por isso quero agradecer primeiramente a Deus, que me deu forças para continuar diante das dificuldades apresentadas.

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

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

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

Agradeço aos amigos que fiz em Rio Claro em especial ao Antônio Nilson, Renato Super, Olívio, Erica, Carlos, Caritá, Leandro, Mariana e meus colegas de classe pelas horas de estudo, apoio e alegria.

Agradeço a todos os meus amigos da Rep JAnelas, em especial ao Virso, Farofa, Tanabi, Xiu, Pinda, Xupeta, Frota, Danado, Panda, Dersão, Brunão, Dan, Ghai, Giba, Hectin, Larika, Madruga, Mané, Marcão Renofio, Nando, Perdido, Porva, Kobal, Tigrão, Xupim, Miguel, Bruninho, Bag, Robinho e a todos os agregados pela amizade, pelos conselhos e por tudo que vocês representaram nessa etapa.

Agradeço aos meus amigos de Ribeirão Preto em especial ao Manoel Balotelli, Nemoto, Brunin Tata, Nanzin, Diguin, Vavá, Ryko, Bill, Boldrin e Daniela Nemoto pelas horas de risos, danone e amizade.

Aos meus pais Marcos e Cleide, ao meu irmão José Marcos, a minha cunhada Thalita e ao meu sobrinho Hugo, que apesar das dificuldades que encontrei, sempre estiveram ao meu lado me apoiando e aconselhando, com muito amor e carinho, para que eu pudesse concluir essa importante etapa da minha vida.

Enfim, agradeço a todas as pessoas que contribuíram para esta realização.

Resumo

Neste trabalho é feito um estudo sobre tópicos de Teoria dos Números Algébricos como extensão de corpos, decomposição de ideais primos, corpos quadráticos e ciclotômicos, número de classe e unidade. Nosso principal objetivo é apresentar uma aplicação dessa teoria na construção de reticulados e solução de equações diofantinas.

Palavras-chave: Extensões de Corpos, Número de Classe, Ideais Primos, Base Integral, Unidades.

Abstract

This work presents a study of topics in algebraic number theory as field extensions, prime ideal decomposition, quadratic and cyclotomic fields, class number and units. Our main goal is to present an application of this theory in the construction of lattices and solution of Diophantine equations.

Keywords: Fields Extensions, Class Number, Prime Ideals, Integral Basis, Units.

Sumário

1 Introdução

Entre os anos de 1808 e 1825, o matemático alemão Carl F. Gauss investigava questões relacionadas à reciprocidade cúbica e à reciprocidade biquadrática em $\mathbb{Z}$, o conjunto dos números inteiros, quando percebeu que essa investigação se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$ do que em $\mathbb{Z}$, em que $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Gauss descobriu que muito da antiga teoria de Euclides sobre fatoração de inteiros poderia ser transportada para $\mathbb{Z}[i]$ com consequências importantes para a Teoria dos Números. O uso que Gauss fez desse novo tipo de número foi de fundamental importância na demonstração do último Teorema de Fermat.

Os números complexos que são raízes de um polinômio mônico com coeficientes inteiros são chamados de números inteiros algébricos. A generalização da noção de número inteiro para número inteiro algébrico dá exemplos especiais de desenvolvimento de uma teoria mais complexa que chamamos de Teoria dos Números Algébricos. Uma grande parte da Teoria dos Números Algébricos desenvolveu-se por meio das tentativas de solução da equação diofantina, mais conhecida como Equação de Fermat

$$x^n + y^n = z^n,$$

pois os inteiros algébricos aparecem de maneira natural, como ferramenta para tratar desse problema. Portanto a busca pela solução da equação de Fermat avançou de sua área de origem, a Teoria dos Números, para uma diferente área de estudo, a Teoria dos Números Algébricos.

Os anéis de inteiros algébricos representam o conceito central da Teoria dos Números Algébricos. Um corpo de números, $\mathbb{K}$, é um subcorpo do corpo dos números complexos que, quando visto como um espaço vetorial sobre os racionais, $\mathbb{Q}$, possui dimensão finita. Os inteiros algébricos contidos em $\mathbb{K}$ formam um anel $\mathcal{O}_{\mathbb{K}}$, que é a estrutura adequada para a generalização da fatoração única em números primos. Em linhas gerais: se α é um número algébrico arbitrário e tomamos o corpo $\mathbb{K} = \mathbb{Q}(\alpha)$ então se considera o subanel $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{K}$ denominado de anel dos inteiros algébricos de $\mathbb{K}$. Os elementos de $\mathcal{O}_{\mathbb{K}}$ são números complexos contidos em $\mathbb{K} = \mathbb{Q}(\alpha)$ que são soluções de equações polinomiais do tipo $x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$, onde todos os coeficientes $a_{n-1}, ..., a_1, a_0$ são números inteiros.

Observe que a relação entre $\mathcal{O}_{\mathbb{K}}$ e $\mathbb{K}$ é análoga à relação entre $\mathbb{Z}$ e $\mathbb{Q}$. Contudo, a

fatoração em primos costuma falhar para elementos do anel de inteiros, mas não falha para ideais. A teoria dos ideais de anéis de inteiros algébricos foi criada para fornecer novos métodos de resolução de problemas clássicos da Teoria dos Números.

Uma grande parte da Teoria dos Números clássica pode ser expressa no contexto da Teoria dos Números Algébricos e essa teoria passou de ferramenta a objeto de investigação essencial na Teoria dos Números. Esse ponto de vista foi bastante enfatizado pelo matemático alemão David Hilbert (1862-1943) que teve uma enorme influência no desenvolvimento na Teoria dos Números. Como resultado, a Teoria dos Números Algébricos é um ramo próspero da Matemática, com aplicações não somente na própria Teoria dos Números. Algumas aplicações da teoria dos números algébricos e que podem ser encontradas em [14] são:

1. **Fatoração de inteiros usando o crivo de um corpo de números:** O crivo de um corpo de números é o algoritmo assintoticamente mais rápido conhecido para fatorar inteiros muito grandes. Em 12 de dezembro de 2009, o crivo de um corpo de números foi usado para fatorar o RSA-768, que tem 232 dígitos decimais e pode ser fatorado como o produto de dois números primos:

   RSA-768 = 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3.

   n = 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489.

   m = 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917.

   $n \cdot m = RSA$-768.

2. **Teste de primalidade**: Agrawal e seus alunos Saxena e Kayal da Índia recentemente (2002) encontraram o primeiro teste de primalidade em tempo polinomial determinístico (no número de dígitos). Neste teste, existem métodos aritméticos que envolvem quocientes de $(\mathbb{Z}/n\mathbb{Z})[x]$, que são melhores compreendidos no contexto da teoria dos números algébricos.

3. **Questões interessantes**:

(a) A Equação de Pell ($x^2 - dy^2 = 1$) pode ser reinterpretada em termos de unidades em corpos quadráticos reais, o que leva a um estudo dos grupos de unidades de corpos de números.

(b) A Fatoração de inteiros leva a fatoração de ideias diferentes de zero em anéis de inteiros de corpos de números.

(c) A teoria de corpos de classe utilizando a demonstração da lei da reciprocidade quadrática de Gauss em termos da aritmética dos corpos ciclotômicos $\mathbb{Q}(e^{2\pi i/n})$.

4. **Demonstração do último teorema de Fermat por Andrew Wiles**: A demonstração de que $x^n + y^n = z^n$ não tem soluções inteiras não triviais usa métodos de teoria dos números algébricos extensivamente (além de muitas outras técnicas). Tentativas de provar o último Teorema de Fermat há muito tempo tiveram grande influência no desenvolvimento da teoria dos números algébricos (por Dedekind, Kummer, Kronecker, entre outros).

5. **Geometria aritmética**: Este é um campo que estuda soluções para equações polinomiais que se encontram em anéis aritmeticamente interessantes, como os inteiros ou inteiros algébricos. Um importante triunfo da geometria aritmética é a prova feita por Faltings da conjectura de Mordell:

   Seja X uma curva plana algébrica sobre um corpo de números $\mathbb{K}$. Assuma que a variedade de $X(\mathbb{C})$ de soluções complexas para X tem pelo menos gênero 2 (i.e., $X(\mathbb{C})$ é topologicamente uma rosca com dois buracos). Então o conjunto de $X(\mathbb{K})$ dos pontos em X com coordenadas em $\mathbb{K}$ é finito.

   Por exemplo, para qualquer $n \geq 4$ e qualquer corpo de números $\mathbb{K}$, existe somente um número finito de soluções em $\mathbb{K}$ para $x^n + y^n = 1$.

6. **Construção de reticulados**: Nos últimos anos, a Teoria dos Números Algébricos tem sido a base do estudo de códigos corretores de erros e reticulados. Dado um ideal no anel dos inteiros algébricos de um corpo de números, tem-se que a imagem deste ideal via o homomorfismo canônico é um reticulado no $\mathbb{R}^n$ chamado de reticulado algébrico.

7. **Aplicações a equações diofantinas**: A equação $y^2 = x^3 + k$, $k \in \mathbb{Z}$, pode ser resolvida usando números algébricos.

Visto que a teoria dos números algébricos pode ser aplicada em diferentes contextos, neste trabalho focamos nas aplicações 6 e 7. Com isso, este trabalho visa mostrar não somente o ferramental teórico sobre Teoria dos Números Algébricos, mas também sua aplicabilidade, possibilitando que pesquisas futuras se beneficiem das informações contidas aqui, indo de encontro com os ideais de formação de um matemático do Programa de Pós-Graduação em Matemática da UNESP - Rio Claro.

Mais especificamente, este trabalho está organizado como se segue.

No Capítulo 2, apresentamos alguns conceitos de extensões de corpos, grau de extensão, elemento algébrico, polinômio minimal, traço, norma, base integral e discriminante que são de fundamental importância para a construção de reticulados.

No Capítulo 3, trabalhamos algumas propriedades de corpos quadráticos e de corpos ciclotômicos, caracterizando sua base integral, anel de inteiros e discriminante.

No Capítulo 4, descrevemos os conceitos de ideais, ideal principal, norma de um ideal, domínio de Dedekind e número de classe. Em destaque temos a fatoração única de ideais, onde todo ideal próprio não nulo em um domínio de Dedekind é representado como um produto de ideais primos.

No Capítulo 5, abordamos como a teoria dos números algébricos pode ser usada na construção de reticulados. Para tanto, apresentamos os conceitos de reticulado, região fundamental, volume da região fundamental, determinante do reticulado, empacotamento esférico e resultados sobre reticulados algébricos.

No Capítulo 6, aplicamos a teoria dos números algébricos para resolver a equação diofantina $y^2 = x^3 + k$. Para tanto usamos os conceitos de número de classe, fatoração de ideais, entre outros.

Os pré-requisitos básicos para um melhor entendimento deste trabalho são: Álgebra Linear, Álgebra, Teoria dos Números e alguns resultados sobre Teoria de Galois, que podem ser consultados nas referências [4], [5], [12], [16].

No decorrer do trabalho, seguem alguns resultados sem demonstração. Alguns por se tratarem de resultados clássicos e outros por apresentarem uma demonstração muito complexa e que foge do escopo desse trabalho. No entanto, no início de cada capítulo colocamos a referência em que esta pode ser encontrada.

2 Extensões de Corpos

Neste capítulo apresentamos os conceitos de extensões de corpos e alguns resultados importantes como o Teorema da multiplicatividade dos graus e o Teorema do Elemento Primitivo. Apresentamos também os números algébricos, que são as raízes de um polinômio com coeficientes em um corpo. O uso que Gauss fez desse novo tipo de número foi de fundamental importância na demonstração do último Teorema de Fermat. Por fim, veremos os conceitos de traço, norma, base integral e discriminante, estes serão importantes no Capítulo 5, onde faremos um estudo sobre reticulados.

As principais referências utilizadas foram [6], [8], [9] e [15].

2.1 Extensões e Elemento Algébrico

Nesta seção apresentamos os conceitos de extensões de corpos e elemento algébrico. Além disso, apresentamos alguns resultados envolvendo estes conceitos.

Definição 2.1. *Sejam* $\mathbb{K}$, $\mathbb{L}$ *corpos. Dizemos que* $\mathbb{L}$ *é uma* ***extensão*** *de* $\mathbb{K}$ *se* $\mathbb{K} \subset \mathbb{L}$. *Notação:* $\mathbb{L}/\mathbb{K}$.

Observação 2.1. Seja $\mathbb{K} \subset \mathbb{L}$ uma extensão de corpos. Pode-se verificar que $\mathbb{L}$ é um $\mathbb{K}$-espaço vetorial, assim, existe uma base de $\mathbb{L}$ sobre $\mathbb{K}$.

Definição 2.2. *Seja* $\mathbb{K} \subset \mathbb{L}$ *uma extensão de corpos.*

(i) A dimensão do $\mathbb{K}$*-espaço vetorial* $\mathbb{L}$ *é o número de elementos da base de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *chamada de* ***grau da extensão*** *de* $\mathbb{L}$ *sobre* $\mathbb{K}$ *e denotada por* $[\mathbb{L} : \mathbb{K}]$.

(ii) Dizemos que $\mathbb{L}$ *é uma extensão finita de* $\mathbb{K}$ *se* $[\mathbb{L} : \mathbb{K}]$ *é finito, caso contrário* $\mathbb{L}$ *é uma extensão infinita.*

Definição 2.3. *Um* ***corpo de números*** $\mathbb{K}$ *é uma extensão finita de* $\mathbb{Q}$.

Teorema 2.1. *(Teorema da multiplicatividade dos graus) Se* $\mathbb{K}$, $\mathbb{M}$ *e* $\mathbb{L}$ *são corpos tais que* $[\mathbb{L} : \mathbb{K}]$ *é finita e* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, *então,* $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}] \cdot [\mathbb{M} : \mathbb{K}]$.

Demonstração. Suponha $[\mathbb{L} : \mathbb{M}] = m$ e $[\mathbb{M} : \mathbb{K}] = n$. Sejam $B_1 = \{\alpha_1, \ldots, \alpha_m\}$ uma base de $\mathbb{L}$ sobre $\mathbb{M}$ e $B_2 = \{\beta_1, \ldots, \beta_n\}$ uma base de $\mathbb{M}$ sobre $\mathbb{K}$.

Afirmação: $B = \{\alpha_i\beta_j, i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ é uma base de $\mathbb{L}/\mathbb{K}$.

1. O conjunto gerado por B, $[B]$, é $\mathbb{L}$. De fato,

   $\alpha \in \mathbb{L} \Rightarrow \exists\, a_1, a_2, \cdots, a_m \in \mathbb{M}$ tais que $\alpha = \sum_{i=1}^{m} a_i\alpha_i$.

   Por outro lado,

   $a_i \in \mathbb{M} \Rightarrow \exists\, b_{i1}, b_{i2}, \cdots, b_{in} \in \mathbb{K}$ tais que $a_i = \sum_{j=1}^{n} b_{ij}\beta_j$.

   Logo, $\alpha = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}\alpha_i\beta_j$. Portanto $\mathbb{L} \subset [B]$ e como $[B] \subset \mathbb{L}$, concluímos que $[B] = \mathbb{L}$.

2. B é linearmente independente sobre $\mathbb{K}$.

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

   Como B_1 é linearmente independente sobre $\mathbb{M}$, temos $\sum_{j=1}^{n} b_{ij}\beta_j = 0$, mas B_2 é linearmente independente sobre $\mathbb{K}$ e assim $b_{ij} = 0, \forall i, j$.

   Portanto B é uma base de $\mathbb{L}/\mathbb{K}$ com mn elementos. Consequentemente pela Definição (2.2),

$$[\mathbb{L} : \mathbb{K}] \overset{(1)e(2)}{=} mn = [\mathbb{L} : \mathbb{M}].[\mathbb{M} : \mathbb{K}].$$

□

Definição 2.4. *Chamamos de* ***corpo de decomposição*** *de um polinômio $f(x) \in \mathbb{K}[x]$ sobre $\mathbb{K}$ o menor subcorpo de $\mathbb{C}$ que contém $\mathbb{K}$ e todas as raízes distintas $\alpha_1, \cdots, \alpha_r$ de $f(x)$ em $\mathbb{C}$.*
Notação: $\mathbb{K}(\alpha_1, \cdots, \alpha_r)$.

Exemplo 2.1. Vejamos como encontrar $\left[\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right]$.

Afirmação I : $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

De fato,

1. $\{1, \sqrt{2}\}$ gera $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$.

   Pode-se mostrar que $\mathbb{Q}(\sqrt{2}) = \{x \mid x = \alpha + \beta\sqrt{2}, \alpha, \beta \in \mathbb{Q}\}$, então $\forall x \in \mathbb{Q}(\sqrt{2}), x = \alpha.1 + \beta\sqrt{2}, \alpha, \beta \in \mathbb{Q}$, ou seja, x é combinação linear de $\{1, \sqrt{2}\}$.

2. $\{1, \sqrt{2}\}$ é linearmente independente sobre $\mathbb{Q}$.

   Suponha que $\alpha.1 + \beta\sqrt{2} = 0, \alpha, \beta, \in \mathbb{Q}$. Se $\beta \neq 0$, então $\sqrt{2} = \dfrac{-\alpha}{\beta}$, o que é absurdo pois $\sqrt{2}$ é irracional. Portanto, $\beta = 0$ e daí temos que $\alpha.1 + 0.\sqrt{2} = 0 \Rightarrow \alpha = 0$. Dessa forma, $\{1, \sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$. Logo $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Afirmação II : $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$.

1. De fato, $\{1, \sqrt{3}\}$ gera $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$.

   Pode-se mostrar que $\mathbb{Q}(\sqrt{3}, \sqrt{2}) = \{x \mid x = \alpha + \beta\sqrt{3}, \alpha, \beta \in \mathbb{Q}(\sqrt{2})\}$, então $\forall x \in \mathbb{Q}(\sqrt{3}, \sqrt{2}), x = \alpha.1 + \beta\sqrt{3}, \alpha, \beta \in \mathbb{Q}(\sqrt{2})$, ou seja, x é combinação linear de $\{1, \sqrt{3}\}$.

2. $\{1, \sqrt{3}\}$ é linearmente independente sobre $\mathbb{Q}(\sqrt{2})$.

   Suponha que $\alpha.1 + \beta\sqrt{3} = 0, \alpha, \beta, \in \mathbb{Q}(\sqrt{2})$. Assim podemos reescrever a igualdade como

$$(p + q\sqrt{2}) + (r + s\sqrt{2})\sqrt{3} = 0,\ p, q, r, s \in \mathbb{Q}.$$

   Se $\beta = (r + s\sqrt{2}) \neq 0$, então

$$\begin{aligned}
\sqrt{3} &= \frac{-(p + q\sqrt{2})}{r + s\sqrt{2}} \\
&= \frac{-(p + q\sqrt{2})}{r + s\sqrt{2}} \cdot \frac{r - s\sqrt{2}}{r - s\sqrt{2}} \\
&= \frac{-(pr - ps\sqrt{2} + qr\sqrt{2} - 2qs)}{r^2 - 2s^2} \\
&= \frac{-pr + 2qs + (ps - qr)\sqrt{2}}{r^2 - 2s^2} \\
&= \frac{-pr + 2qs}{r^2 - 2s^2} + \frac{(ps - qr)\sqrt{2}}{r^2 - 2s^2} \\
&= a + b\sqrt{2},\ a, b \in \mathbb{Q}.
\end{aligned}$$

   Assim,

$$\begin{aligned}
(\sqrt{3})^2 &= (a + b\sqrt{2})^2 \\
3 &= a^2 + 2ab\sqrt{2} + 2b^2 \\
3 - a^2 - 2b^2 &= 2ab\sqrt{2} \\
\frac{3 - a^2 - 2b^2}{2ab} &= \sqrt{2},
\end{aligned} \tag{2.1}$$

o que é absurdo pois $\sqrt{2}$ é irracional. Portanto, $r + s\sqrt{2} = \beta = 0$ e daí temos que $p + q\sqrt{2} + 0.\sqrt{3} = 0 \Rightarrow p + q\sqrt{2} = \alpha = 0$. Dessa forma, $\{1, \sqrt{3}\}$ é uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}(\sqrt{2})$. Logo $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

Pelo Teorema da multiplicatividade dos graus,

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})].[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.2 = 4$$

e $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ é uma base de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ sobre $\mathbb{Q}$.

Definição 2.5. *Seja $\mathbb{K}$ um corpo qualquer. Chamamos de* ***polinômio*** *sobre $\mathbb{K}$ em uma indeterminada x a uma expressão formal $p(x) = a_0 + a_1x + ... + a_mx^m + ...$ onde $a_i \in \mathbb{K}, \forall\ i \in \mathbb{N}$ e existe $n \in \mathbb{N}$ tal que $a_j = 0,\ \forall\ j > n$ e $a_n \neq 0$. O grau de $p(x)$ é definido como n.*

Denotamos por $\mathbb{K}[x]$ o ***conjunto de todos os polinômios*** *sobre $\mathbb{K}$, em uma indeterminada x.*

Observe que não está definido o grau do polinômio 0 e considere ∂ como uma função do conjunto de todos os polinômios $\neq 0$ no conjunto $\mathbb{N}$ definida por

$$\begin{aligned} \partial : \mathbb{K}[x] - \{0\} &\rightarrow \mathbb{N} \\ p(x) &\mapsto \partial p(x) = \textit{grau de } p(x) \end{aligned}$$

Definição 2.6. *Seja $f(x) \in \mathbb{K}[x]$ tal que $\partial f(x) \geq 1$. Dizemos que $f(x)$ é um* ***polinômio irredutível*** *sobre $\mathbb{K}$ se toda vez que $f(x) = g(x) \cdot h(x); g(x), h(x) \in \mathbb{K}[x]$ então temos $g(x) = a$ constante em $\mathbb{K}$ ou $h(x) = b$ constante em $\mathbb{K}$. Se $f(x)$ for não irredutível sobre $\mathbb{K}$ dizemos que f é redutível sobre $\mathbb{K}$.*

Definição 2.7. *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos. Um elemento $\alpha \in \mathbb{L}$ é chamado de* ***algébrico*** *sobre $\mathbb{K}$ se existe $f(x) \in \mathbb{K}[x] \setminus \{0\}$ tal que $f(\alpha) = 0$. O polinômio irredutível e mônico de menor grau $f(x)$ tal que $f(\alpha) = 0$ é chamado de* ***polinômio minimal*** *de α sobre $\mathbb{K}$ e é denotado por $min_{\mathbb{K}}\alpha$.*

Definição 2.8. *Uma extensão $\mathbb{L}$ sobre $\mathbb{K}$ é* ***algébrica*** *se todo $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$.*

Exemplo 2.2. Vamos verificar que a extensão $\mathbb{Q}(\sqrt{2})$ sobre $\mathbb{Q}$ é algébrica.

$$\alpha \in \mathbb{Q}(\sqrt{2}) \Rightarrow \alpha = a + b\sqrt{2}, a, b \in \mathbb{Q} \Rightarrow (\alpha - a)^2 = 2b^2 \Rightarrow \alpha^2 - 2a\alpha + a^2 - 2b^2 = 0.$$

Logo, α é raiz de $f(x) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x]$ e dessa forma, α é algébrico sobre $\mathbb{Q}$. Portanto, a extensão $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ é algébrica.

Definição 2.9. *Dizemos que α é* ***inteiro algébrico*** *se existe $f(x) \in \mathbb{Z}[x]^* = \mathbb{Z}[x]\setminus\{0\}$, mônico, tal que $f(\alpha) = 0$. O conjunto $\mathcal{O}_{\mathbb{K}} = \{\alpha \in \mathbb{K} \mid \alpha$ é inteiro algébrico $\}$ é um anel chamado* ***anel dos inteiros de*** *$\mathbb{K}$.*

Exemplo 2.3. O elemento $\alpha = \sqrt{2} + \sqrt{3}$ é inteiro algébrico, pois é raiz do polinômio $x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$.

Definição 2.10. *Um* ***domínio*** *A é um anel comutativo com identidade 1_A que satisfaz a seguinte propriedade:*

$$a, b \in A;\ ab = 0 \Rightarrow a = 0 \textit{ ou } b = 0.$$

Definição 2.11. *Sejam A um domínio e $\mathbb{K} = \left\{\frac{a}{s}; a, s \in A, s \neq 0\right\}$ o corpo das frações de A. Dizemos que A é* ***integralmente fechado*** *se $\mathcal{O}_{\mathbb{K}} = A$.*

Teorema 2.2. *[15] Se $\mathbb{L} \supset \mathbb{K} \supset \mathbb{Q}$, $[\mathbb{L} : \mathbb{K}] < \infty$. Então existe $\theta \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\theta)$. O elemento θ é chamado* ***elemento primitivo****.*

Proposição 2.1. *[15] Seja $\mathbb{K}$ é um corpo de números tal que $\mathbb{L} = \mathbb{K}(\theta)$, então $[\mathbb{L} : \mathbb{K}] = \partial(min_{\mathbb{K}}\theta)$.*

Exemplo 2.4. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, então $[\mathbb{K} : \mathbb{Q}] = 2$ pois $min_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$.

Observação 2.2. Se $\mathbb{L} = \mathbb{K}(\theta)$ e $\partial(min_{\mathbb{K}}\theta) = n$, então $\mathbb{K}(\theta) = \{a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}; a_i \in \mathbb{K}, \forall\ i = 0, 1, \cdots, n-1\}$.

Definição 2.12. *Sejam $\mathbb{K} \subset \mathbb{L}$ corpos. Dizemos que $\mathbb{L}/\mathbb{K}$ é uma* ***extensão de Galois*** *se existe $f(x) \in \mathbb{K}[x]$ tal que $\mathbb{L} = \mathbb{K}(R_f)$, onde R_f denota as raízes de f.*

Exemplo 2.5. A extensão do Exemplo 2.4 é uma extensão de Galois, pois $\mathbb{K} = \mathbb{Q}(\sqrt{2}, -\sqrt{2})$.

Definição 2.13. *Seja $\mathbb{L}$ uma extensão de $\mathbb{K}$. O* ***grupo de Galois*** *de $\mathbb{L}$ sobre $\mathbb{K}$ é dado por*

$$Gal(\mathbb{L}/\mathbb{K}) = \{\sigma \in Aut(\mathbb{L});\ \sigma(x) = x,\ \forall x \in \mathbb{K}\}\,.$$

Teorema 2.3. *[8] Se $\mathbb{K} = \mathbb{Q}(\theta)$ é uma extensão de $\mathbb{Q}$ de grau n, então existem exatamente n monomorfismos distintos $\{\sigma_1, ..., \sigma_n\}$ de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$. Tais monomorfismos são dados por $\sigma_i(\theta) = \theta_i$, em que $\{\theta_1, ..., \theta_n\}$ são as raízes de $min_{\mathbb{Q}}\theta$ em $\mathbb{C}$.*

Exemplo 2.6. Considere o corpo $\mathbb{Q}(\sqrt[3]{2})$. O polinômio minimal de $\sqrt[3]{2}$ sobre $\mathbb{Q}$ é $f(x) = x^3 - 2$. Se $\sigma : \mathbb{K} \to \mathbb{C}$ é um monomorfismo que fixa $\mathbb{Q}$, então $\sigma(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\sigma(\sqrt[3]{2}) + c(\sigma(\sqrt[3]{2}))^2$. Portanto, para saber quem é σ, basta definir σ em $\sqrt[3]{2}$.

Temos que as raízes de $f(x)$ são $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$, em que $\omega = cos\left(\frac{2\pi}{n}\right) + isen\left(\frac{2\pi}{n}\right)$. Assim temos três monomorfismos:

$$\begin{array}{rccc} \sigma_1(x): & \mathbb{Q}(\sqrt[3]{2}) & \longrightarrow & \mathbb{C} \\ & \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \end{array}$$

$$\begin{array}{rccc} \sigma_2(x): & \mathbb{Q}(\sqrt[3]{2}) & \longrightarrow & \mathbb{C} \\ & \sqrt[3]{2} & \longmapsto & \omega\sqrt[3]{2} \end{array}$$

$$\begin{array}{rccc} \sigma_3(x): & \mathbb{Q}(\sqrt[3]{2}) & \longrightarrow & \mathbb{C} \\ & \sqrt[3]{2} & \longmapsto & \omega^2\sqrt[3]{2} \end{array}$$

Definição 2.14. *Sejam $\mathbb{K}$ um corpo de números de grau n e $\{\sigma_1, ..., \sigma_n\}$ os n $\mathbb{Q}$-monomorfismos distintos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{Q}$. Dizemos que o monomorfismo σ_i é* ***real*** *se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, caso contrário, dizemos que σ_i é* ***imaginário****. Além disso, se todos os $\sigma_i's$, para $i = 1, ..., n$, são reais, dizemos que o corpo $\mathbb{K}$ é* ***totalmente real*** *e, se todos os $\sigma_i's$, para $i = 1, ..., n$ são imaginários, dizemos que $\mathbb{K}$ é* ***totalmente imaginário****.*

Definição 2.15. *Seja $\mathbb{K}/\mathbb{F}$ uma extensão de corpos. Se σ é um monomorfismo de $\mathbb{K}$ tal que $\sigma(\alpha) = \alpha$ para todo $\alpha \in \mathbb{F}$, então σ é chamado de* ***$\mathbb{F}$-monomorfismo*** *de $\mathbb{K}$. Se σ é um $\mathbb{F}$-automorfismo de $\mathbb{K} = \mathbb{F}(\alpha)$ então $\sigma(\alpha)$ é chamado de* ***conjugado*** *de α sobre $\mathbb{F}$.*

Observação 2.3. Todo monomorfismo de $\mathbb{F}$ em $\mathbb{C}$ estende a exatamente $[\mathbb{E} : \mathbb{F}]$ monomorfismos de $\mathbb{E}$ em $\mathbb{C}$. Daí conclui-se que o número de $\mathbb{F}$-isomorfismos de $\mathbb{E}$ é $[\mathbb{E} : \mathbb{F}]$.

2.2 Traço e Norma

Nesta seção vamos introduzir alguns conceitos que serão cruciais para o desenvolvimento da teoria de base integral e discriminante que será abordada na Seção 2.3.

Definição 2.16. *Seja $\mathbb{F}$ um corpo de números de grau n e seja σ_j para $j = 1, 2, ..., n$ os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$. Para cada elemento $\alpha \in \mathbb{F}$,*

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha),$$

é chamado de ***traço*** *de α sobre $\mathbb{F}$ e, também, temos que*

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) = \prod_{j=1}^{n} \sigma_j(\alpha),$$

é chamado de ***norma*** *de α sobre $\mathbb{F}$.*

Exemplo 2.7. Sejam $\mathbb{F} = \mathbb{Q}(\sqrt{13})$, $\alpha = 1+\sqrt{13}$ e $\beta = (3+\sqrt{13})/2$. Os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são

$$\begin{array}{rccc} \sigma_1 : & \mathbb{Q}(\sqrt{13}) & \to & \mathbb{C} \\ & \sqrt{13} & \mapsto & \sqrt{13} \end{array} \qquad \begin{array}{rccc} \sigma_2 : & \mathbb{Q}(\sqrt{13}) & \to & \mathbb{C} \\ & \sqrt{13} & \mapsto & -\sqrt{13} \end{array}$$

e os elementos de $\mathbb{Q}$ ficam fixos. Segue que

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (1 + \sqrt{13})(1 - \sqrt{13}) = -12,$$

$$N_{\mathbb{F}/\mathbb{Q}}(\beta) = \sigma_1(\beta)\sigma_2(\beta) = \left(\frac{3 + \sqrt{13}}{2}\right)\left(\frac{3 - \sqrt{13}}{2}\right) = -1,$$

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (1+\sqrt{13}) + (1-\sqrt{13}) = 2$$

e

$$Tr_{\mathbb{F}/\mathbb{Q}}(\beta) = \sigma_1(\beta) + \sigma_2(\beta) = \frac{3+\sqrt{13}}{2} + \frac{3-\sqrt{13}}{2} = 3.$$

E também, temos

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha\beta) = N_{\mathbb{F}/\mathbb{Q}}\left((1+\sqrt{13})\left(\frac{3+\sqrt{13}}{2}\right)\right) = N_{\mathbb{F}/\mathbb{Q}}(8+2\sqrt{13}) = \sigma_1(8+2\sqrt{13})\sigma_2(8+2\sqrt{13}) =$$

$$(8+2\sqrt{13})(8-2\sqrt{13}) = 8^2 - 4.13 = 12 = (-12)(-1) = N_{\mathbb{F}/\mathbb{Q}}(\alpha)N_{\mathbb{F}/\mathbb{Q}}(\beta)$$

e

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha+\beta) = Tr_{\mathbb{F}/\mathbb{Q}}\left((1+\sqrt{13}) + \left(\frac{3+\sqrt{13}}{2}\right)\right) = Tr_{\mathbb{F}/\mathbb{Q}}\left(\frac{5+3\sqrt{13}}{2}\right) =$$

$$= \sigma_1\left(\frac{5+3\sqrt{13}}{2}\right) + \sigma_2\left(\frac{5+3\sqrt{13}}{2}\right) = 5 = 2+3 = Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) + Tr_{\mathbb{F}/\mathbb{Q}}(\beta).$$

Este exemplo ilustra algumas propriedades de traço e norma apresentadas a seguir.

Sejam $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$ corpos, onde $\mathbb{K} \subseteq \mathbb{L}$ é uma extensão finita. Se $\alpha, \alpha' \in \mathbb{L}$ e $a \in \mathbb{K}$, então valem as seguintes propriedades:

1. $Tr_{\mathbb{L}/\mathbb{K}}(\alpha+\alpha') = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\alpha')$;
2. $Tr_{\mathbb{L}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{L}/\mathbb{K}}(\alpha)$;
3. $Tr_{\mathbb{L}/\mathbb{K}}(a) = [\mathbb{L}:\mathbb{K}]a$;
4. $N_{\mathbb{L}/\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$;
5. $N_{\mathbb{L}/\mathbb{K}}(a\alpha) = a^{[\mathbb{L}:\mathbb{K}]}N_{\mathbb{L}/\mathbb{K}}(\alpha)$;
6. $N_{\mathbb{L}/\mathbb{K}}(\alpha\alpha') = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\alpha')$.

Vamos definir agora norma e traço para extensões relativas.

Definição 2.17. *Sejam $\mathbb{K}/\mathbb{F}$ uma extensão de corpos com $[\mathbb{K}:\mathbb{F}] = n$ e σ_j para $j = 1, 2, ..., n$ todos os $\mathbb{F}$-monomorfismo de $\mathbb{K}$. Seja $\alpha \in \mathbb{K}$, definimos*

$$N_{\mathbb{K}/\mathbb{F}}(\alpha) = \prod_{j=1}^{n} \sigma_j(\alpha),$$

é chamado de ***norma relativa*** *de* α *em* $\mathbb{K}/\mathbb{F}$. *Ainda,*

$$Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = \sum_{j=1}^{n} \sigma_j(\alpha),$$

é chamado de ***traço relativo*** *de* α *em* $\mathbb{K}/\mathbb{F}$.

Observe que quando $\mathbb{F} = \mathbb{Q}$, *essas noções coincidem com os indicados na Definição 2.16 e neste caso chamamos* $N_{\mathbb{K}/\mathbb{Q}}$ *de* ***norma absoluta*** *e* $Tr_{\mathbb{K}/\mathbb{Q}}$ *de* ***traço absoluto***.

Exemplo 2.8. Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$ e $\mathbb{F} = \mathbb{Q}(\sqrt{3})$. Os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ que fixam $\mathbb{F}$ são

$$\begin{array}{rccc} \sigma_1: & \mathbb{K} & \to & \mathbb{C} \\ & \sqrt{-1} & \mapsto & \sqrt{-1} \end{array} \qquad \begin{array}{rccc} \sigma_2: & \mathbb{K} & \to & \mathbb{C} \\ & \sqrt{-1} & \mapsto & -\sqrt{-1} \end{array}$$

Tome $\alpha = 5 + \sqrt{-1} \in \mathbb{K}$. Segue que

$$N_{\mathbb{K}/\mathbb{F}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = (5 + \sqrt{-1})(5 - \sqrt{-1}) = 26$$

e

$$Tr_{\mathbb{K}/\mathbb{F}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (5 + \sqrt{-1}) + (5 - \sqrt{-1}) = 10.$$

Teorema 2.4. *[8] Se* $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ *é uma torre de corpos de números, então para* $\alpha \in \mathbb{L}$ *temos o seguinte:*

(a) $N_{\mathbb{L}/\mathbb{F}}(\alpha) = N_{\mathbb{K}/\mathbb{F}}(N_{\mathbb{L}/\mathbb{K}}(\alpha))$ *e* $N_{\mathbb{L}/\mathbb{F}}(\alpha) \in \mathbb{F}$.

(b) $Tr_{\mathbb{L}/\mathbb{F}}(\alpha) = Tr_{\mathbb{K}/\mathbb{F}}(Tr_{\mathbb{L}/\mathbb{K}}(\alpha))$ *e* $Tr_{\mathbb{L}/\mathbb{F}}(\alpha) \in \mathbb{F}$.

(c) Se $[\mathbb{L} : \mathbb{F}(\alpha)] = r$, *então*

$$N_{\mathbb{L}/\mathbb{F}}(\alpha) = (N_{\mathbb{F}(\alpha)/\mathbb{F}}(\alpha))^r \text{ e } Tr_{\mathbb{L}/\mathbb{F}}(\alpha) = r(Tr_{\mathbb{F}(\alpha)/\mathbb{F}}(\alpha)).$$

Demonstração.

(a) Sejam σ_j, $j = 1, 2, ..., n = [\mathbb{L} : \mathbb{K}]$ elementos dos $\mathbb{K}$-monomorfismos de $\mathbb{L}$ e seja ψ_k, $k = 1, 2, ..., m = [\mathbb{K} : \mathbb{F}]$ elementos dos $\mathbb{F}$-monomorfismos de $\mathbb{K}$. Então

$$N_{\mathbb{K}/\mathbb{F}}(N_{\mathbb{L}/\mathbb{K}}(\alpha)) = \prod_{k=1}^{m} \psi_k \left(\prod_{j=1}^{n} \sigma_j(\alpha) \right) = \prod_{k=1}^{m} \prod_{j=1}^{n} \psi_k(\sigma_j(\alpha)) = N_{\mathbb{L}/\mathbb{F}}(\alpha),$$

uma vez que $\psi_k\sigma_j$ são todos distintos e incluem os $\mathbb{F}$-monomorfismos de $\mathbb{L}$. Observe que se ψ_1 é o monomorfismo identidade de $\mathbb{K}$, então σ_j restrito a $\mathbb{K}$ é igual a ψ_1, isto é, $\sigma_j|_{\mathbb{K}} = \psi_1$ para todo $j = 1, 2, ..., n$ e que ψ_k estende a n monomorfismos de $\mathbb{L}$ sobre $\mathbb{C}$ para cada $k = 1, 2, ..., m$.

(b) A propriedade para o traço é provada de forma semelhante a prova de (a), empregando adição no lugar de multiplicação.

(c) Estas fórmulas são provadas da mesma maneira que será dada na demonstração do Teorema 2.5. □

Exemplo 2.9. Sejam $\mathbb{L} = \mathbb{Q}(\sqrt{5}, \sqrt{-1}), \mathbb{K} = \mathbb{Q}(\sqrt{-1})$ e $\mathbb{F} = \mathbb{Q}$.

Se $\alpha = \sqrt{5} + \sqrt{-1}$, então

$$N_{\mathbb{K}/\mathbb{F}}(N_{\mathbb{L}/\mathbb{K}}(\alpha)) = N_{\mathbb{K}/\mathbb{F}}((\sqrt{5} + \sqrt{-1})(-\sqrt{5} + \sqrt{-1})) = N_{\mathbb{K}/\mathbb{F}}(-6) = 36 =$$

$$(\sqrt{5} + \sqrt{-1})(-\sqrt{5} + \sqrt{-1})(\sqrt{5} - \sqrt{-1})(-\sqrt{5} - \sqrt{-1}) = N_{\mathbb{L}/\mathbb{F}}(\alpha).$$

Temos, também

$$Tr_{\mathbb{K}/\mathbb{F}}(Tr_{\mathbb{L}/\mathbb{K}}(\alpha)) = Tr_{\mathbb{K}/\mathbb{F}}((\sqrt{5} + \sqrt{-1}) + (-\sqrt{5} + \sqrt{-1})) = Tr_{\mathbb{K}/\mathbb{F}}(2\sqrt{-1}) =$$

$$2\sqrt{-1} - 2\sqrt{-1} = 0 = (\sqrt{5} + \sqrt{-1}) + (-\sqrt{5} + \sqrt{-1}) + (\sqrt{5} - \sqrt{-1}) + (-\sqrt{5} - \sqrt{-1}) = Tr_{\mathbb{L}/\mathbb{F}}(\alpha).$$

Se $\beta = 3 + \sqrt{-1}$, então

$$N_{\mathbb{L}/\mathbb{F}}(\beta) = (N_{\mathbb{K}/\mathbb{F}}(\beta))^2 = 10^2 = 100$$

e

$$Tr_{\mathbb{L}/\mathbb{F}}(\beta) = 2Tr_{\mathbb{K}/\mathbb{F}}(\beta) = 2.6 = 12.$$

Teorema 2.5. *[8] (Propriedades de norma e traço em subcorpos)*

Sejam $\mathbb{F}$ um corpo de números de grau n e $\alpha \in \mathbb{F}$ com $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$. Se $\alpha = \alpha_1, \alpha_2, ..., \alpha_d$ são todos os conjugados de α sobre $\mathbb{Q}$, ou seja, as raízes de $min_{\mathbb{Q}}\alpha$, então

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) = \frac{n}{d}\sum_{j=1}^{d}\alpha_j = \frac{n}{d}Tr_{\mathbb{Q}(\alpha)}(\alpha)$$

e

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) = \left(\prod_{j=1}^{d}\alpha_j\right)^{n/d} = (N_{\mathbb{Q}(\alpha)}(\alpha))^{n/d}.$$

Além disso,

$$min_{\mathbb{Q}}\alpha = x^d - Tr_{\mathbb{Q}(\alpha)}(\alpha)x^{d-1} + ... \pm N_{\mathbb{Q}(\alpha)}(\alpha).$$

Demonstração. Considere os monomorfismos de $\mathbb{Q}(\alpha)$ em $\mathbb{C}$ que fixam $\mathbb{Q}$ dados por

$$\sigma_j(\alpha) \mapsto \alpha_j \quad (1 \leq j \leq d),$$

onde $\sigma_j(q) = q$ para todo $q \in \mathbb{Q}$. Então pela Definição 2.16,

$$Tr_{\mathbb{Q}(\alpha)}(\alpha) = \sum_{j=1}^{d} \alpha_j \text{ e } N_{\mathbb{Q}(\alpha)}(\alpha) = \prod_{j=1}^{d} \alpha_j.$$

Pela Observação 2.3, cada um dos σ_i, para $i = 1, 2, ..., d$, estende a exatamente n/d monomorfismos de $\mathbb{F}$ em $\mathbb{C}$, que vamos denotar por

$$\sigma_i^{(j)}, \text{ para } j = 1, 2, ..., n/d.$$

Portanto,

$$Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) = \sum_{i=1}^{d} \sum_{j=1}^{n/d} \sigma_i^{(j)}(\alpha) = \sum_{i=1}^{d} \frac{n}{d} \alpha_i = \frac{n}{d} \sum_{i=1}^{d} \alpha_i$$

e

$$N_{\mathbb{F}/\mathbb{Q}}(\alpha) = \prod_{i=1}^{d} \prod_{j=1}^{n/d} \sigma_i^{(j)}(\alpha) = \prod_{i=1}^{d} \alpha_i^{n/d} = \left(\prod_{i=1}^{d} \alpha_i \right)^{n/d}.$$

Finalmente, na expansão de

$$min_{\mathbb{Q}}\alpha = \prod_{i=1}^{d} (x - \alpha_i),$$

vemos que o termo constante deve ser

$$\pm \prod_{i=1}^{d} \alpha_i = \pm N_{\mathbb{Q}(\alpha)}(\alpha),$$

enquanto que o coeficiente x^{d-1} deve ser

$$-\sum_{i=1}^{d} \alpha_i = -Tr_{\mathbb{Q}(\alpha)}(\alpha).$$

Isso completa a demonstração.

□

Corolário 2.1. *Se $\mathbb{F}$ é um corpo de números e $\alpha \in \mathbb{F}$, então*

$$Tr_{\mathbb{F}}(\alpha) \in \mathbb{Q} \text{ e } N_{\mathbb{F}}(\alpha) \in \mathbb{Q}.$$

Corolário 2.2. *Se $\alpha \in \mathbb{F}$ é um inteiro algébrico então $N_{\mathbb{F}/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ e $Tr_{\mathbb{F}/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.*

Exemplo 2.10. Considere o polinômio quadrático irredutível

$$f(x) = ax^2 + bx + c \in \mathbb{Q}[x],$$

onde $a \neq 0$. As raízes de $f(x)$ são dadas por

$$\alpha = \frac{-b+\sqrt{\Delta}}{2a} \quad e \quad \alpha^{'} = \frac{-b-\sqrt{\Delta}}{2a},$$

onde $\Delta = b^2 - 4ac$ é o discriminante do corpo quadrático $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{\Delta})$. Portanto,

$$Tr_{\mathbb{F}}(\alpha) = Tr_{\mathbb{Q}(\alpha)}(\alpha) = \alpha + \alpha^{'} = \frac{-b+\sqrt{\Delta}}{2a} + \frac{-b-\sqrt{\Delta}}{2a} = -b/a$$

e

$$N_{\mathbb{F}}(\alpha) = N_{\mathbb{Q}(\alpha)}(\alpha) = \alpha\alpha^{'} = \left(\frac{-b+\sqrt{\Delta}}{2a}\right)\left(\frac{-b-\sqrt{\Delta}}{2a}\right) = \frac{b^2-\Delta}{4a^2} = c/a.$$

Assim, o polinômio minimal de α sobre $\mathbb{Q}$ é $min_{\mathbb{Q}}\alpha = x^2 - Tr_{\mathbb{F}}(\alpha)x + N_{\mathbb{F}}(\alpha)$.

Definição 2.18. *Um elemento α de um domínio A é chamado de* ***unidade*** *se α divide 1.*

Proposição 2.2. *Um inteiro algébrico x é uma unidade em $\mathbb{K}$ se, e somente se, $N_{\mathbb{K}}(x) = \pm 1$.*

Demonstração. Se x é uma unidade, então existe um inteiro algébrico x' tal que $xx' = 1$. Assim

$$N_{\mathbb{K}}(xx') = N_{\mathbb{K}}(x)N_{\mathbb{K}}(x') = N_{\mathbb{K}}(1) = 1,$$

e deste modo, $N_{\mathbb{K}}(x)$ é uma unidade em $\mathbb{Z}$, e portanto, $N_{\mathbb{K}}(x) = \pm 1$.

Reciprocamente, se $N_{\mathbb{K}}(x) = \pm 1$, ou seja, $N_{\mathbb{K}}(x) = \prod x^{(i)} = \pm 1$. Assim fazendo

$$x' = x^{(2)}x^{(3)}, \cdots, x^{(n)}$$

segue que $1 = N_{\mathbb{K}}(x) = xx'$, e como x' é um inteiro algébrico, segue que x divide 1 em $\mathcal{O}_{\mathbb{K}}$. Portanto, x' é uma unidade em $\mathcal{O}_{\mathbb{K}}$. □

2.3 Base Integral e Discriminante

Nesta seção, apresentamos os conceitos de base integral, discriminante e alguns resultados como o determinante de Vandermonde, que serão de muita importância para a construção de reticulados no Capítulo 5.

Definição 2.19. *Se $\mathcal{O}_{\mathbb{F}}$ é o anel de inteiros de um corpo de números $\mathbb{F}$, uma base de $\mathcal{O}_{\mathbb{F}}$ sobre $\mathbb{Z}$, ou simplesmente uma $\mathbb{Z}$-base para $\mathcal{O}_{\mathbb{F}}$, é chamada de uma* ***base integral*** *para $\mathcal{O}_{\mathbb{F}}$.*

Observação 2.4. 1. Todo corpo de números $\mathbb{K}$ possui uma base integral,[15].

2. Para definição de $\mathbb{Z}$-base consultar [15].

Exemplo 2.11. Se $\mathbb{F} = \mathbb{Q}(\sqrt{13})$, veremos no próximo capítulo que

$$\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[(1+\sqrt{13})/2] = \left\{ a + b\left(\frac{1+\sqrt{13}}{2}\right); a, b \in \mathbb{Z} \right\} \neq \mathbb{Z}[\sqrt{13}] = \{a+b\sqrt{13}; a, b \in \mathbb{Z}\}.$$

Veja que $\alpha = (1+\sqrt{13})/2$ é uma raiz de $min_{\mathbb{Q}}\alpha(x) = x^2 - x - 3$, enquanto que $\beta = \sqrt{13}$ é uma raiz de $x^2 - 13$. Apesar de $\{1, \beta\}$ ser uma base para $\mathbb{F}$ contendo inteiros algébricos, ela não é uma base integral para $\mathbb{F}$.

Definição 2.20. *Seja $\mathbb{F} = \mathbb{Q}(\alpha)$ um corpo de números com $[\mathbb{F} : \mathbb{Q}] = d$. Se*

$$\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_d\}$$

é uma $\mathbb{Q}$-base para $\mathbb{F}$ e σ_j $(1 \leq j \leq d)$ são todos monomorfismos de $\mathbb{F}$ em $\mathbb{C}$, então o ***discriminante*** *da base $\mathcal{B}$ é dado por*

$$\mathcal{D}(\mathcal{B}) = (det(\sigma_j(\alpha_i)))^2,$$

onde det é o determinante da matriz com entradas $\sigma_j(\alpha_i)$ na i-ésima linha e j-ésima coluna.

Em particular, se

$$\mathcal{B} = \{1, \alpha, ..., \alpha^{d-1}\},$$

então o determinante da matriz $(\sigma_j(\alpha^{i-1}))$ é chamado de ***determinante de Vandermonde*** *e seu valor é*

$$det(\sigma_j(\alpha^{i-1})) = \prod_{1 \leq i < j \leq d} (\alpha_j - \alpha_i), \tag{2.2}$$

onde $\alpha_k = \sigma_k(\alpha)$ é um k-ésimo conjugado de α, para $k = 1, 2, ..., d$.

Exemplo 2.12. Se $\mathbb{F} = \mathbb{Q}(\sqrt{2})$ veremos no Capítulo 3 que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Z}\}$ e $\mathcal{B} = \{1, \sqrt{2}\}$ é uma base integral de $\mathbb{F}$. Os $\mathbb{Q}$-monomorfismos de $\mathbb{F}$ em $\mathbb{C}$ são dados por:

$$\sigma_1 : \sqrt{2} \mapsto \sqrt{2} \text{ e } \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}.$$

Portanto,

$$\mathcal{D}(\mathcal{B}) = (det(\sigma_j(\alpha^{i-1})))^2 = \left(det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{2}) & \sigma_2(\sqrt{2}) \end{pmatrix} \right)^2 =$$

$$= \left(det \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix} \right)^2 = (-2\sqrt{2})^2 = 8.$$

Proposição 2.3. *Sejam $\mathbb{K}$ um corpo, $\mathbb{L} = \mathbb{K}(\alpha)$ uma extensão finita de $\mathbb{K}$ de grau n e $f(x)$ o polinômio minimal de α sobre $\mathbb{K}$. Então,*

$$\mathcal{D}_{\mathbb{L}/\mathbb{K}}(1, \alpha, ..., \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(f'(\alpha)),$$

onde $f'(\alpha)$ é a derivada de $f(x)$ em α.

Demonstração. Sejam $\alpha_1, ..., \alpha_n$ as raízes de $f(x)$ em alguma extensão de $\mathbb{K}$ e $\sigma_i, i = 1, ..., n$ os monomorfismos de $\mathbb{L}$ em $\mathbb{C}$. Temos que $\mathcal{D}_{\mathbb{L}/\mathbb{K}}(1, \alpha, ..., \alpha^{n-1}) = (det(\sigma_i(\alpha^j)))^2 = det(\alpha_i^j)^2$, com $i = 1, ..., n$ e $j = 0, ..., n-1$. Como $det(\alpha_i^j)$ é um determinante de Vandermonde, segue que

$$(det(\alpha_i^j))^2 = \left[\prod_{1 \le k < i \le n} (\alpha_i - \alpha_k)\right]^2 = \prod_{1 \le k < i \le n} [(\alpha_i - \alpha_k)(\alpha_i - \alpha_k)] =$$

$$= (-1)^{\frac{1}{2}n(n-1)} \prod_{1 \le k < i \le n, i \ne k} (\alpha_i - \alpha_k) = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} \left[\prod_{k=1, k \ne 1}^{n} (\alpha_i - \alpha_k)\right] =$$

$$= (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{1}{2}n(n-1)} N(f'(\alpha)),$$

o que prova a proposição. □

Teorema 2.6. *[8] Se $\mathcal{B}_1 = \{\alpha_1, \alpha_2, ..., \alpha_d\}$ e $\mathcal{B}_2 = \{\beta_1, \beta_2, ..., \beta_d\}$ são duas $\mathbb{Q}$-bases para um corpo de números $\mathbb{F}$, então*

$$\mathcal{D}(\mathcal{B}_2) = d^2 \mathcal{D}(\mathcal{B}_1),$$

onde $d = det(q_{k,i}) \in \mathbb{Q}$, $d \ne 0$, e $q_{k,i} \in \mathbb{Q}$ é determinado por

$$\beta_k = \sum_{i=1}^{d} q_{k,i} \alpha_i, \qquad (q_{k,i} \in \mathbb{Q}).$$

Além disso, $d \in \mathbb{Z}$ desde que $\mathcal{B}_1$ seja uma base integral e $\mathcal{B}_2 \in \mathcal{O}_{\mathbb{F}}$.

Demonstração. Seja σ_j, $(1 \le j \le d)$ os monomorfismos de $\mathbb{F}$ em $\mathbb{C}$. A representação $\beta_k = \sum_{i=1}^{d} q_{k,i} \alpha_i$, implica que

$$\sigma_j(\beta_k) = \sum_{i=1}^{d} q_{k,i} \sigma_j(\alpha_i),$$

para cada $k = 1, 2, ..., d$. Assim, temos uma equação matricial

$$\begin{pmatrix} \sigma_1(\beta_1) & \sigma_2(\beta_1) & \dots & \sigma_d(\beta_1) \\ \sigma_1(\beta_2) & \sigma_2(\beta_2) & \dots & \sigma_d(\beta_2) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\beta_d) & \sigma_2(\beta_d) & \dots & \sigma_d(\beta_d) \end{pmatrix} =$$

$$\begin{pmatrix} q_{1,1} & q_{1,2} & \dots & q_{1,d} \\ q_{2,1} & q_{2,2} & \dots & q_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ q_{d,1} & q_{d,2} & \dots & q_{d,d} \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \dots & \sigma_d(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \dots & \sigma_d(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_d) & \sigma_2(\alpha_d) & \dots & \sigma_d(\alpha_d) \end{pmatrix}.$$

Tomando os determinantes e elevando ao quadrado, obtemos a equação:

$$\mathcal{D}(\mathcal{B}_2) = d^2\mathcal{D}(\mathcal{B}_1),$$

com $d = det(M)$, onde

$$M = \begin{pmatrix} q_{1,1} & q_{1,2} & \dots & q_{1,d} \\ q_{2,1} & q_{2,2} & \dots & q_{2,d} \\ \vdots & \vdots & \vdots & \vdots \\ q_{d,1} & q_{d,2} & \dots & q_{d,d} \end{pmatrix}.$$

□

Exemplo 2.13. Sejam $\mathbb{F} = \mathbb{Q}(\sqrt{13})$, $\alpha = (1+\sqrt{13})/2$ e $\beta = \sqrt{13}$. No Exemplo 2.11, vimos que $\mathcal{B}_1 = \{1, \alpha\}$ e $\mathcal{B}_2 = \{1, \beta\}$ são bases para $\mathbb{F}$, sendo a primeira integral, e a última não integral, mas apenas uma base sobre $\mathbb{Q}$. Como

$$\sigma_1 : \sqrt{13} \mapsto \sqrt{13}, \;\; e \;\; \sigma_2 : \sqrt{13} \mapsto -\sqrt{13}$$

são os $\mathbb{Q}$-monomorfismos de $\mathbb{F}$ em $\mathbb{C}$, segue que

$$\mathcal{D}(\mathcal{B}_2) = (det(\sigma_j(\beta^i)))^2 = \left(det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{13}) & \sigma_2(\sqrt{13}) \end{pmatrix} \right)^2$$

$$= \left(det \begin{pmatrix} 1 & 1 \\ \sqrt{13} & -\sqrt{13} \end{pmatrix} \right)^2 = (-2\sqrt{13})^2 = 52$$

e

$$\mathcal{D}(\mathcal{B}_1) = (det(\sigma_j(\alpha^i)))^2 = \left(det \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{13}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{13}}{2}\right) \end{pmatrix} \right)^2$$

$$= \left(det \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{13}}{2} & \frac{1-\sqrt{13}}{2} \end{pmatrix} \right)^2 = (-\sqrt{13})^2 = 13.$$

Assim,

$$\mathcal{D}(\mathcal{B}_2) = d^2\mathcal{D}(\mathcal{B}_1) = 2^2\mathcal{D}(\mathcal{B}_1).$$

Portanto,

$$d = det \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} = 2,$$

pois

$$\beta_1 = 1 = q_{1,1}.\alpha_1 + q_{1,2}.\alpha_2 = 1.1 + 0.\frac{1+\sqrt{13}}{2},$$

e

$$\beta_2 = \sqrt{13} = q_{2,1}.\alpha_1 + q_{2,2}.\alpha_2 = -1.1 + 2.\frac{1+\sqrt{13}}{2}.$$

Teorema 2.7. *[8] Se $\mathcal{B} = \{\alpha_1, \alpha_2, ..., \alpha_d\}$ é uma $\mathbb{Q}$-base para um corpo de números $\mathbb{F} = \mathbb{Q}(\alpha)$, então*

$$\mathcal{D}(\mathcal{B}) = det(Tr_{\mathbb{F}}(\alpha_i\alpha_j)) \in \mathbb{Q},$$

e $\mathcal{D}(\mathcal{B}) \neq 0$. Além disso, se $\mathbb{F}$ é um corpo totalmente real, então $\mathcal{D}(\mathcal{B}) > 0$.

Demonstração. Como $\mathcal{D}(\mathcal{B}) = det(\sigma_j(\alpha_i))^2$, segue pelas propriedades de determinante que:

$$(det(\sigma_j(\alpha_i)))^2 = det\left(\sum_{k=1}^{d} \sigma_k(\alpha_i\alpha_j)\right) = det(Tr_{\mathbb{F}}(\alpha_i\alpha_j)),$$

logo $\mathcal{D}(\mathcal{B}) = det(Tr_{\mathbb{F}}(\alpha_i\alpha_j))$. Portanto, pelo Corolário 2.1, $\mathcal{D}(\mathcal{B}) \in \mathbb{Q}$.

Resta mostrar que $\mathcal{D}(\beta)$ é diferente de zero e também positiva quando $\mathbb{F}$ é totalmente real.

Seja $\mathcal{B}_1 = \mathcal{B}$. Pelo Teorema 2.2,

$$\mathcal{B}_2 = \{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$$

é uma base para $\mathbb{F}$ sobre $\mathbb{Q}$. Assim, pelo Teorema 2.6, $\mathcal{D}(\mathcal{B}_2) = d^2\mathcal{D}(\mathcal{B}_1)$, onde d é dado no Teorema 2.6.

No entanto, por (2.2)

$$\mathcal{D}(\mathcal{B}_2) = \prod_{1\leq i<j\leq d} (\alpha_j - \alpha_i)^2,$$

e os α_i são distintos de forma que $\mathcal{D}(\mathcal{B}_2) \neq 0$. Assim, $\mathcal{D}(\mathcal{B}_1) \neq 0$.

Sendo que $\mathcal{B}_2$ é uma base para $\mathbb{F}$ sobre $\mathbb{Q}$, então pelo Teorema 2.6,

$$\mathcal{D}(\mathcal{B}_1) = d_1^2\mathcal{D}(\mathcal{B}_2).$$

Portanto, $\mathcal{D}(\mathcal{B}_2)$ é um quadrado. Como $\mathcal{D}(\mathcal{B}_1) \neq 0$, se $\mathbb{F}$ é totalmente real, então todos os α_j são reais e portanto $\mathcal{D}(\mathcal{B}_1) > 0$. □

Corolário 2.3. *Se $\mathcal{B}$ é uma base de $\mathbb{F}$ sobre $\mathbb{Q}$ com $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{F}}$, então $\mathcal{D}(\mathcal{B}) \in \mathbb{Z}$.*

Demonstração. Como $\mathcal{D}(\mathcal{B}) = det(Tr_{\mathbb{F}}(\alpha_i\alpha_j))$ onde $\mathcal{B} = \{\alpha_1, ..., \alpha_d\}$ é uma base de $\mathbb{F}$ sobre $\mathbb{Q}$ segue, pelo Corolário 2.2, que $\mathcal{D}(\mathcal{B}) \in \mathbb{Z}$. □

Exemplo 2.14. Vimos no Exemplo 2.13 que o corpo totalmente real $\mathbb{F} = \mathbb{Q}(\sqrt{13})$ possui base integral

$$\mathcal{B}_1 = \{1, (1+\sqrt{13})/2\} = \{1, \alpha\} = \{\alpha_1, \alpha_2\}$$

e uma $\mathbb{Q}$ -base não integral é

$$\mathcal{B}_2 = \{1, \sqrt{13}\} = \{1, \beta\} = \{\beta_1, \beta_2\}.$$

Além disso, seja a matriz

$$Tr_{\mathbb{F}}(\alpha_i\alpha_j) = \begin{pmatrix} Tr_{\mathbb{F}}(1) & Tr_{\mathbb{F}}(\alpha) \\ Tr_{\mathbb{F}}(\alpha) & Tr_{\mathbb{F}}(\alpha^2) \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix},$$

então

$$\mathcal{D}(\mathcal{B}_1) = det(Tr_{\mathbb{F}}(\alpha_i\alpha_j)) = det \begin{pmatrix} 2 & 1 \\ 1 & 7 \end{pmatrix} = 13 \in \mathbb{Z}.$$

Além disso, uma vez que temos a matriz

$$Tr_{\mathbb{F}}(\beta_i\beta_j)) = \begin{pmatrix} Tr_{\mathbb{F}}(1) & Tr_{\mathbb{F}}(\beta) \\ Tr_{\mathbb{F}}(\beta) & Tr_{\mathbb{F}}(\beta^2) \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 26 \end{pmatrix},$$

então

$$\mathcal{D}(\mathcal{B}_2) = 52 = det(Tr_{\mathbb{F}}(\beta_i\beta_j)) \in \mathbb{Z}.$$

Corolário 2.4. *[8] Seja $\mathcal{B}_1 = \{\alpha_1, \alpha_2, ..., \alpha_d\}$ uma $\mathbb{Q}$-base para o corpo de números $\mathbb{F}$. Se $\mathcal{B}_2 = \{\beta_1, \beta_2, ..., \beta_d\} \subseteq \mathbb{F}$ e*

$$\beta_k = \sum_{i=1}^{d} q_{k,i}\alpha_i \text{ para } q_{k,i} \in \mathbb{F}, \text{ e } k = 1, 2, ..., d,$$

então $\mathcal{B}_2$ é uma base para $\mathbb{F}$ se, e somente se, $det(q_{k,i}) \neq 0$.

Demonstração. Suponha que $det(q_{k,i}) \neq 0$. É suficiente mostrar que os β_k são linearmente independentes. Se

$$\sum_{k=1}^{d} \gamma_k\beta_k = 0 \qquad (\gamma_k \in \mathbb{F}),$$

então

$$0 = \sum_{k=1}^{d} \gamma_k \sum_{i=1}^{d} q_{k,i}\alpha_i = \sum_{i=1}^{d} \alpha_i \sum_{k=1}^{d} \gamma_k q_{k,i}.$$

Uma vez que os α_i são linearmente independentes, segue que

$$\sum_{k=1}^{d} \gamma_k q_{k,i} = 0.$$

Seja $det(q_{k,i}) \neq 0$, então $\gamma_k = 0$ para todo $k = 1, 2, ..., d$. Por outro lado, se $\mathcal{B}_2$ é uma base para $\mathbb{F}$, então pelo Teorema 2.6,

$$\mathcal{D}(\mathcal{B}_2) = d^2 \mathcal{D}(\mathcal{B}_1).$$

Assim, pelo Teorema 2.7 segue o resultado. □

O próximo teorema dá um modo de sabermos quando uma base é integral. Antes de enunciá-lo precisamos saber quando um inteiro é livre de quadrados

Definição 2.21. *Dizemos que $n \in \mathbb{Z}$ é **livre de quadrados** se, e somente se, n não tem divisor que é o quadrado de um número primo. Ou seja, se, e somente se, p é primo tal que*

$$p^2 \mid n \Rightarrow p^2 = 1$$

Teorema 2.8. *[8] Se $\mathcal{B} \subseteq \mathcal{O}_{\mathbb{F}}$ é uma $\mathbb{Q}$-base para $\mathbb{F}$ e $\mathcal{D}(\mathcal{B})$ é livre de quadrados, então $\mathcal{B}$ é uma base integral para $\mathbb{F}$.*

Exemplo 2.15. O Exemplo 2.11 fornece um exemplo de um discriminante livre de quadrados de uma base integral. No entanto, $\mathcal{B} = \{1, \sqrt{2}\}$ é uma base integral para $\mathbb{Q}(\sqrt{2})$ mas $\mathcal{D}(\mathcal{B}) = 8$, portanto o inverso do Teorema 2.8 não é verdadeiro.

Embora o Exemplo 2.15 mostra que o inverso do Teorema 2.8 não é verdadeiro, podemos mostrar que se temos duas bases integrais para um corpo de números, então elas devem ter o mesmo discriminante.

Corolário 2.5. *[8] Sejam $\mathcal{B}_1$ e $\mathcal{B}_2$ duas bases integrais para um corpo de números $\mathbb{F}$. Então*

$$\mathcal{D}(\mathcal{B}_1) = \mathcal{D}(\mathcal{B}_2).$$

Demonstração. Pelo Teorema 2.6,

$$\mathcal{D}(\mathcal{B}_2) = d^2 \mathcal{D}(\mathcal{B}_2), \tag{2.3}$$

onde $d \in \mathbb{Z}$ é dado no Teorema 2.6. Assim,

$$\mathcal{D}(\mathcal{B}_1) | \mathcal{D}(\mathcal{B}_2) \in \mathbb{Z},$$

pelo Corolário 2.3. Invertendo os papéis de $\mathcal{B}_1$ e $\mathcal{B}_2$, temos que

$$\mathcal{D}(\mathcal{B}_2)|\mathcal{D}(\mathcal{B}_1) \in \mathbb{Z}.$$

Portanto,

$$\mathcal{D}(\mathcal{B}_1) = \pm\mathcal{D}(\mathcal{B}_2).$$

Consequentemente, pela Equação 2.3, o sinal de subtração não é possível.

□

O Corolário 2.5 nos diz essencialmente que o discriminante de uma base integral para um corpo de números é um invariante do corpo.

No próximo capítulo veremos como encontrar uma base integral e discriminante dos corpos quadráticos e ciclotômicos.

3 Corpos Quadráticos e Ciclotômicos

Neste capítulo apresentamos os conceitos de corpos quadráticos e corpos ciclotômicos. Os corpos quadráticos e ciclotômicos têm muita importância para a Teoria dos Números Algébricos, como por exemplo na construção de reticulados que será abordada no Capítulo 5 e também para a solução de equação Diofantina que será abordada no Capítulo 6. Os corpos ciclotômicos desempenham um papel fundamental na Teoria dos Números Algébricos, por causa da sua relação com o último Teorema de Fermat. Através dos corpos ciclotômicos é possível caracterizar o anel dos inteiros, o discriminante e obter reticulados.

As principais referências utilizadas foram [6], [7], [8], [10], [11] e [17].

3.1 Corpos Quadráticos

Nesta seção apresentamos o conceito de corpos quadráticos e suas propriedades.

Definição 3.1. *Uma extensão de corpos de grau 2 sobre o corpo $\mathbb{Q}$ é chamada um* ***corpo quadrático****.*

Exemplo 3.1. O corpo $\mathbb{L} = \mathbb{Q}(\sqrt{13})$ é um corpo quadrático, pois $\theta = \sqrt{13}$ é um zero do polinômio $f(x) = x^2 - 13 \in \mathbb{Q}[x]$.

Proposição 3.1. *[10] Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados.*

Demonstração. Sejam $\mathbb{K} = \mathbb{Q}(\theta)$ um corpo quadrático e $f(x) = x^2 + ax + b$, com $a, b \in \mathbb{Q}$, o polinômio minimal de $\theta \in \mathbb{K}$. Resolvendo a equação quadrática $\theta^2 + a\theta + b = 0$, temos que $\theta = \dfrac{-a \pm \sqrt{a^2 - 4b}}{2}$ são as raízes de $f(x)$. Como $2\theta \pm a = \sqrt{a^2 - 4b}$, segue que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b})$.

Por outro lado, $a^2 - 4b$ é um número racional que podemos escrever como $a^2 - 4b = \dfrac{u}{v} = \dfrac{uv}{v^2}$, com $u, v \in \mathbb{Z}$ e $mdc(u, v) = 1$ e de forma que u e v não sejam quadrados perfeitos, pois caso contrário teríamos $\mathbb{Q}(\theta) = \mathbb{Q}$. Assim, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b}) = \mathbb{Q}\left(\sqrt{\dfrac{u}{v}}\right) = \mathbb{Q}\left(\sqrt{\dfrac{uv}{v^2}}\right) = \mathbb{Q}(\sqrt{uv})$. Suponhamos que $uv = k^2 d$, com $k, d, \in \mathbb{Z}$, e d livre de quadrados. Logo, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{uv}) = \mathbb{Q}(\sqrt{k^2 d}) = \mathbb{Q}(\sqrt{d})$.

□

Observação 3.1. Se $d > 0$, a extensão $\mathbb{Q}(\sqrt{d})$ é **totalmente real** e se $d < 0$, a extensão $\mathbb{Q}(\sqrt{d})$ é **totalmente imaginária**.

A Proposição a seguir é compatível com o Corolário 2.2, vamos apresentar uma demonstração no caso em que o corpo é quadrático.

Proposição 3.2. *[11] Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados, um corpo quadrático. Se um elemento $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ é um inteiro algébrico, então $2a$ e $a^2 - db^2$ são números inteiros.*

Demonstração. Seja $\alpha \in \mathbb{K}$ um inteiro algébrico. Então existem $a_0, \cdots, a_{n-1} \in \mathbb{Z}$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Assim, considerando σ o automorfismo de $\mathbb{K}$ tal que $\sigma(\sqrt{d}) = -\sqrt{d}$, segue que, $\sigma(\alpha)^n + a_{n-1}\sigma(\alpha)^{n-1} + \cdots + a_1\sigma(\alpha) + a_0 = 0$, ou seja, $\sigma(\alpha)$ também é um inteiro algébrico de $\mathbb{K}$. Temos que $\alpha + \sigma(\alpha)$ e $\alpha\sigma(\alpha)$ também são inteiros algébricos de $\mathbb{K}$. Além disso, se $\alpha = a + b\sqrt{d}$, com a, $b \in \mathbb{Q}$, então $\alpha + \sigma(\alpha) = 2a \in \mathbb{Q}$ e $\alpha\sigma(\alpha) = a^2 - db^2 \in \mathbb{Q}$. Como $\mathbb{Z}$ é integralmente fechado segue que $2a$ e $a^2 - db^2$ são números inteiros. □

A seguir determinaremos o anel dos inteiros algébricos de um corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados, para isso sejam $\mathbb{Z}[d] = \{a + b\sqrt{d}; a, b \in \mathbb{Z}\}$ e $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right); a, b \in \mathbb{Z}\right\}$.

Teorema 3.1. *[15] Se $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ é um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados, então o anel dos inteiros algébricos $\mathcal{O}_{\mathbb{K}}$ de $\mathbb{Q}(\sqrt{d})$ é dado por:*
a) $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$ *se* $d \equiv 2 (mod\, 4)$ *ou* $d \equiv 3 (mod\, 4)$ *e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é* $\{1, \sqrt{d}\}$;
b) $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$ *se* $d \equiv 1 (mod\, 4)$ *e uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ é* $\{1, \frac{1+\sqrt{d}}{2}\}$.

Demonstração. Seja $\alpha = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, com a, $b \in \mathbb{Q}$, um inteiro algébrico sobre $\mathbb{Z}$.

Se $b = 0$ então o polinômio minimal de α sobre $\mathbb{Q}$ é dado por $min_{\mathbb{Q}}(x) = x - a$, e como α é um inteiro algébrico sobre $\mathbb{Z}$, segue que $a \in \mathbb{Z}$.

Se $b \neq 0$, então o polinômio minimal $min_{\mathbb{Q}}(x)$ de α sobre $\mathbb{Q}$ tem grau 2 e é obtido do seguinte modo:

$$\alpha = a + b\sqrt{d} \Longrightarrow \alpha - a = b\sqrt{d} \Longrightarrow (\alpha - a)^2 = b^2 d \Longrightarrow \alpha^2 - 2a\alpha + a^2 = b^2 d \Longrightarrow$$
$$\alpha^2 - 2a\alpha + (a^2 - b^2 d) = 0.$$

Logo $min_{\mathbb{Q}}(x) = x^2 - 2ax + a^2 - db^2$. Pela Proposição 3.2 sabemos que $2a$, $a^2 - db^2 \in \mathbb{Z}$. Assim, $(2a)^2 - d(2b)^2 \in \mathbb{Z}$ e daí $d(2b)^2 \in \mathbb{Z}$, pois $2a \in \mathbb{Z}$. Ainda temos que $2b \in \mathbb{Z}$, pois, caso contrário, no seu denominador existiria um fator primo p que apareceria na forma p^2 no denominador de $(2b)^2$ e como d é livre de quadrados teríamos que $d(2b)^2 \notin \mathbb{Z}$, o que é um absurdo.

Logo, $2b \in \mathbb{Z}$ e podemos escrever:

$$a = \frac{u}{2},\ b = \frac{v}{2},\quad com\, u,\ v \in \mathbb{Z}. \tag{3.1}$$

Além disso,

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z}. \tag{3.2}$$

Substituindo a por $\frac{u}{2}$ e b por $\frac{v}{2}$, obtemos $u^2 - dv^2 \in\ 4\mathbb{Z}$.

a) Se $d \equiv 2(mod\,4)$ ou $d \equiv 3(mod\,4)$, então u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1(mod\,4)$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$ segue que $u^2 \equiv dv^2 \equiv d(mod\,4)$, ou seja, $d \equiv 0(mod\,4)$ ou $d \equiv 1(mod\,4)$, o que é um absurdo. Portanto, concluímos que v é par, isto é, $v^2 \equiv 0(mod\,4)$ e assim, $u^2 \equiv dv^2 \equiv 0(mod\,4)$ o que implica que u é par. Logo, se $\alpha = a + b\sqrt{d} \in \mathcal{O}_{\mathbb{K}}$ então $\alpha \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}[\sqrt{d}]$.

Por outro lado, tomando $\alpha \in \mathbb{Z}[\sqrt{d}]$, temos que α é raiz do polinômio $x^2 - 2ax + a^2 - db^2 \in \mathbb{Z}[x]$, pois pela Proposição (3.2), sabemos que $2a,\ a^2 - db^2 \in \mathbb{Z}$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_{\mathbb{K}}$. Portanto, $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{d}]$.

b) Se $d \equiv 1(mod\,4)$, então $u^2 - dv^2 \in 4\mathbb{Z}$, e que u e v são de mesma paridade, isto é, são ambos pares ou ímpares. Se u e v são pares então $a,\ b \in \mathbb{Z}$. Logo, $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $\alpha = a + b\sqrt{d} = u/2 + v/2\sqrt{d} = (u - v)/2 + v((1 + \sqrt{d})/2) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. Portanto, $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, ou seja, $\mathcal{O}_{\mathbb{K}} \subset \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$.

Por outro lado, se $\alpha = a + b\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, com $a,\ b \in \mathbb{Z}$, então $2a + b \in \mathbb{Z}$ e $(a + b/2)^2 - d(b/2)^2 = a^2 + ab + (1 - d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1(mod\,4)$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subset \mathcal{O}_{\mathbb{K}}$, pois os coeficientes do polinômio minimal de α, que é $min_{\mathbb{Q}}(x) = x^2 - (2a + b)x + a^2 + ab + (1 - d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_{\mathbb{K}}$. □

Exemplo 3.2. Seja $\mathbb{K}$ o corpo quadrático $\mathbb{Q}(\sqrt{-1})$. O anel dos inteiros algébricos de $\mathbb{K}$ é dado por $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$ pois $d = -1 \equiv 3(mod\,4)$. O anel dos inteiros algébricos do corpo quadrático $\mathbb{Q}(\sqrt{-3})$ é $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ pois $d = -3 \equiv 1(mod\,4)$.

Proposição 3.3. *Seja d um inteiro livre de quadrados, qualquer discriminante de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$ é dado por:*

(1) $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = d$, *se* $d \equiv 1(mod\ 4)$;

(2) $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = 4d$, *se* $d \equiv 2(mod\ 4)$ *ou* $d \equiv 3(mod\ 4)$.

Demonstração. Como os $\mathbb{Q}$-monomorfismos de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ em $\mathbb{C}$, com $d \in \mathbb{Z}$ livre de quadrados, são σ_1 e σ_2, onde $\sigma_1(\sqrt{d}) = \sqrt{d}$ e $\sigma_2(\sqrt{d}) = -\sqrt{d}$, segue que o discriminante de um corpo quadrático é obtido do seguinte modo:

i) se $d \equiv 1(mod\,4)$, então

$$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{K}/\mathbb{Q}}\left(1, \frac{1+\sqrt{d}}{2}\right) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{d}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{d}}{2}\right) \end{pmatrix}\right)^2 =$$

$$= \left(\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{d}}{2} & \frac{1-\sqrt{d}}{2} \end{pmatrix}\right)^2 = d.$$

ii) se $d \equiv 2(mod\,4)$ ou $d \equiv 3(mod\,4)$ então

$\mathcal{D}_{\mathbb{K}} = \mathcal{D}_{\mathbb{K}/\mathbb{Q}}\left(1, \sqrt{d}\right) = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{d}) & \sigma_2(\sqrt{d}) \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}\right)^2 =$ $4d$. □

Exemplo 3.3. Dado $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, tem-se $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, isto é, $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathcal{O}_{\mathbb{K}}$ e o discriminante de $\mathbb{K}$ é

$$\mathcal{D}_{\mathbb{K}} = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}\right)^2 = 5.$$

Os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são $\sigma_1(a+b\sqrt{5}) = a+b\sqrt{5}$ e $\sigma_2(a+b\sqrt{5}) = a-b\sqrt{5}$. Logo, $Tr_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{5}) = \sum_{i=1}^{2}\sigma_i(a+b\sqrt{5}) = 2a$ e $N_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{5}) = \prod_{i=1}^{2}\sigma_i(a+b\sqrt{5}) = a^2 - 5b^2$.

Exemplo 3.4. Dado $\mathbb{K} = \mathbb{Q}(i)$, então $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-1}]$, isto é, $\{1, \sqrt{-1}\}$ é uma base integral para $\mathcal{O}_{\mathbb{K}}$ e o discriminante absoluto de $\mathbb{K}$ é

$$\mathcal{D}_{\mathbb{K}} = \left(\det\begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1(\sqrt{-1}) & \sigma_2(\sqrt{-1}) \end{pmatrix}\right)^2 = \left(\det\begin{pmatrix} 1 & 1 \\ \sqrt{-1} & -\sqrt{-1} \end{pmatrix}\right)^2 = -4.$$

Os $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$ são $\sigma_1(a+b\sqrt{-1}) = a+b\sqrt{-1}$ e $\sigma_2(a+b\sqrt{-1}) = a-b\sqrt{-1}$. Logo, $Tr_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{-1}) = \sum_{i=1}^{2}\sigma_i(a+b\sqrt{-1}) = 2a$ e $N_{\mathbb{K}/\mathbb{Q}}(a+b\sqrt{-1}) = \prod_{i=1}^{2}\sigma_i(a+b\sqrt{-1}) = a^2+b^2$.

Observação 3.2. No Teorema 2.2 podemos pensar que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha]$ em que $\alpha \in \mathcal{O}_{\mathbb{K}}$ para qualquer corpo de números $\mathbb{K}$. Em outras palavras, podemos ser atraídos a crer que existe sempre uma base integral da forma $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ onde $d = [\mathbb{K} : \mathbb{Q}]$. No entanto, isso é falso como mostra o exemplo a seguir.

Exemplo 3.5. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-7}, \sqrt{-14})$, $\mathbb{F} = \mathbb{Q}(\sqrt{-14})$, e $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\sqrt{-14}]$. Vamos mostrar que não existe $\beta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$. Primeiramente, vamos mostrar que não existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha, \sqrt{-14}]$. Por contradição, suponha que existe um tal α. Então, em particular,

$$k = \frac{1+\sqrt{-7}}{2} = \gamma_1\alpha + \gamma_2, \text{ onde } k \in \mathcal{O}_{\mathbb{K}}, \gamma_1, \gamma_2 \in \mathcal{O}_{\mathbb{F}}.$$

e

$$\sqrt{-14}/\sqrt{-7} = \sqrt{2} = \beta_1\alpha + \beta_2, \text{ onde } \sqrt{2} \in \mathcal{O}_{\mathbb{K}}, \text{ e } \beta_1, \beta_2 \in \mathcal{O}_{\mathbb{F}}.$$

Seja σ o $\mathbb{Q}$-monomorfismo de $\mathbb{K}$ em $\mathbb{C}$ dado por $\sigma : \sqrt{-7} \mapsto -\sqrt{-7}$ e $\sigma : \sqrt{-14} \mapsto \sqrt{-14}$, ou seja, σ fixa os elementos de $\mathbb{F}$. Portanto,

$$\sigma(k) = \frac{1-\sqrt{-7}}{2} = \gamma_1\sigma(\alpha) + \gamma_2,$$
$$k - \sigma(k) = \frac{1+\sqrt{-7}}{2} - \frac{1-\sqrt{-7}}{2} = \sqrt{-7},$$

por outro lado

$$k - \sigma(k) = \gamma_1\alpha + \gamma_2 - (\gamma_1\sigma(\alpha) + \gamma_2) = \gamma_1(\alpha - \sigma(\alpha)).$$

Portanto,

$$k - \sigma(k) = \gamma_1(\alpha - \sigma(\alpha)).$$

Também temos,

$$\sigma(\sqrt{2}) = -\sqrt{2} = \beta_1\sigma(\alpha) + \beta_2,$$
$$\sqrt{2} - \sigma(\sqrt{2}) = \sqrt{2} - \beta_1\sigma(\alpha) + \beta_2 = \sqrt{2} - (-\sqrt{2}) = 2\sqrt{2}.$$

Por outro lado,

$$\sqrt{2} - \sigma(\sqrt{2}) = \beta_1\alpha + \beta_2 - (\beta_1\sigma(\alpha) + \beta_2) = \beta_1(\alpha - \sigma(\alpha)).$$

Portanto,

$$2\sqrt{2} = \beta_1(\alpha - \sigma(\alpha)).$$

Utilizando as igualdades anteriores e norma de $\mathbb{F}$:

$$7^2 = N_{\mathbb{F}}(\gamma_1)^2 N_{\mathbb{F}}(\alpha - \sigma(\alpha))^2 \text{ e } 2^6 = N_{\mathbb{F}}(\beta_1)^2 N_{\mathbb{F}}(\alpha - \sigma(\alpha))^2.$$

Temos que $N_{\mathbb{F}}(\alpha - \sigma(\alpha)) = \pm 1$, uma vez que $N_{\mathbb{F}}(\alpha - \sigma(\alpha)) \in \mathbb{Z}$ e divide 7^2 e 2^6. Assim, $N_{\mathbb{F}}(\gamma_1) = \pm 7$, pois $7^2 = N_{\mathbb{F}}(\gamma_1)^2 N_{\mathbb{F}}(\alpha - \sigma(\alpha))^2$ e $N_{\mathbb{F}}(\alpha - \sigma(\alpha)) = \pm 1$. Porém, $\gamma_1 = a + b\sqrt{-14}$ para algum $a, b \in \mathbb{Z}$, então $N(\gamma_1) = N(a + b\sqrt{-14}) \Rightarrow \pm 7 = a^2 + 14b^2$ o que é impossível. Portanto não existe $\alpha \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha, \sqrt{-14}]$.

Agora se existe um $\beta \in \mathcal{O}_{\mathbb{K}}$ tal que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\beta]$ então definindo $\alpha = \beta - \sqrt{-14}$ segue que $\alpha \in \mathcal{O}_{\mathbb{K}}$ pois $\beta \in \mathcal{O}_{\mathbb{K}}$ e $\sqrt{-14} \in \mathcal{O}_{\mathbb{K}}$, daí obtemos que $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\alpha, \sqrt{-14}]$, o que acabamos de mostrar ser impossível.

3.1.1 Unidades em um Corpo Quadrático

Nesta seção, apresentamos as unidades do anel de inteiros de um corpo quadrático $\mathbb{Q}(\sqrt{d})$, explicitamos as unidades no caso onde d é um inteiro 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.

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro e livre de quadrados. Primeiramente determinamos as unidades de $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, para $d < 0$.

Se $d < 0$ e $d \equiv 2(mod\ 4)$ 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,

$$N_{\mathbb{K}}(\alpha) = \alpha\alpha' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d \geq 1,\ pois\ d < 0.$$

Além disso, x é uma unidade se, e somente se, $N_{\mathbb{K}}(x) = \pm 1$. Como $d < 0$, 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

$$N_{\mathbb{K}}(\alpha) = \alpha\alpha' = \left(\frac{a + b\sqrt{d}}{2}\right)\left(\frac{a - b\sqrt{d}}{2}\right) = \frac{a^2 - b^2 d}{4} \geq 1,\ pois\ d < 0,$$

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

Teorema 3.2. *[1] Seja $\mathbb{K}$ um corpo quadrático imaginário. Então o conjunto das unidades de $\mathcal{O}_{\mathbb{K}}$ é*

$$\begin{cases} \{\pm 1, \pm i\} \simeq \mathbb{Z}_4, & se\ \mathbb{K} = \mathbb{Q}(\sqrt{-1}), \\ \{\pm 1, \pm\omega, \pm\omega^2\} \simeq \mathbb{Z}_6, & se\ \mathbb{K} = \mathbb{Q}(\sqrt{-3}), \\ \{\pm 1\} \simeq \mathbb{Z}_2, & caso\ contrário, \end{cases}$$

onde $\omega = (-1 + \sqrt{-3})/2$.

Demonstração. Para a primeira igualdade, se $d = -1$ então $d \not\equiv 1(mod\ 4)$. Assim, das considerações que precedem o teorema, segue que $\alpha = a + b\sqrt{d}$ é uma unidade se, e somente se, $a^2 + b^2 = 1$. Portanto, $a = 0$ 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 a segunda igualdade, se $d = -3$, então $d \equiv 1(mod\ 4)$. Assim, das considerações que precedem 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 $\alpha = 1, \alpha = -1, \alpha = \frac{1 \pm \sqrt{-3}}{2}$ e $\alpha = \frac{-1 \pm \sqrt{-3}}{2}$ são unidades de $\mathcal{O}_{\mathbb{K}}$, ou seja, $\{\pm 1, \pm\omega, \pm\omega^2\}$.

Para a terceira igualdade, 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 $d' \neq 3$. Se $d' \equiv 2(mod\ 4)$ ou $d' \equiv 3(mod\ 4)$ então 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 unidades de $\mathcal{O}_{\mathbb{K}}$.

b) Se $d' = -d > 0$, então $d' \neq 1$, ou seja, $d' \geq 2$ e $d' \neq 3$. Se $d' \equiv 1(mod\ 4)$ então $d' \geq 5$, 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 $\mathcal{O}_{\mathbb{K}}$. □

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.

Definição 3.2. *A menor unidade $u_1 > 1$ de $\mathcal{O}_{\mathbb{K}}$ é chamada de* ***unidade fundamental*** *do corpo $\mathbb{K}$.*

Precisamos do seguinte teorema:

Teorema 3.3. *[1] Seja d um inteiro positivo livre de quadrados. Então toda unidade de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ é da forma $\pm\eta^n$ $(n \in \mathbb{Z})$, onde η é a unidade fundamental de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Se $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ contém unidades de norma -1 estas são indicadas por $\pm\eta^n$ com n ímpar e as de norma 1 por $\pm\eta^n$ com n par.*

Exemplo 3.6. A determinação da unidade fundamental pode ser feita da seguinte maneira:

1. Caso $d \equiv 2(mod\ 4)$ 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

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

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. Caso $d \equiv 1 (mod\ 4)$. 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

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

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.

Consideremos, 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 $\mathbb{Q}(\sqrt{5})$.

3.2 Corpos Ciclotômicos

Nesta seção apresentamos o conceito de corpos ciclotômicos e suas propriedades.

Definição 3.3. *Seja n um inteiro positivo. Dizemos que ζ_n é uma raiz n-ésima da unidade se $\zeta_n^n = 1$, e que ζ_n é uma raiz n-ésima primitiva da unidade se $\zeta_n^n = 1$ e $\zeta_n^m \neq 1$, para todo $1 \leq m \leq n-1$. O corpo $\mathbb{Q}(\zeta_n)$ é chamado* ***corpo ciclotômico****.*

Observação 3.3. Existem exatamente n raízes n-ésimas distintas da unidade. O conjunto destas raízes $\{\zeta_{n_k} = cos\left(\frac{2k\pi}{n}\right) + isen\left(\frac{2k\pi}{n}\right)$, para $k = 0, 1, ..., n-1\}$ forma um grupo cíclico em relação à multiplicação, tendo ζ_{n_1} como um gerador.

Definição 3.4. *Seja ζ_n uma raiz n-ésima primitiva da unidade. Um corpo ciclotômico $\mathbb{K}$ é a* ***menor extensão*** *de $\mathbb{Q}$ contendo ζ_n, isto é, $\mathbb{K} = \mathbb{Q}(\zeta_n)$.*

Definição 3.5. *O polinômio $\phi_n(x) = \prod_{j=1}^{n}(x - \zeta_n^j)$ é chamado de* ***n-ésimo polinômio ciclotômico****, onde ζ_n^j é uma raiz n-ésima primitiva da unidade, para $j = 1, ..., n$, com $mdc(j, n) = 1$.*

Lema 3.1. *[6] Se n é um inteiro positivo, então $x^n - 1 = \prod_{d|n} \phi_d(x)$.*

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

Segue do Lema 3.1 que $\phi_n(x) = \dfrac{x^n - 1}{\prod_{d|n, d<n} \phi_d(x)}$, $n > 1$ e $\phi_1(x) = x - 1$.

Exemplo 3.7. Se $n = p$, com p um número primo, então

$$\phi_p = \frac{x^p - 1}{x - 1} = x^{p-1} + ... + x + 1$$

é o p-**ésimo polinômio ciclotômico**. Se $n = p^r$, com p um número primo e r um inteiro positivo, então

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

e

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

Logo $\phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = x^{(p-1)p^{r-1}} + x^{(p-2)p^{r-1}} + ... + x^{p^{r-1}} + 1$ é o p^r-**ésimo polinômio ciclotômico**.

Lema 3.2. *[7] Temos que* $\prod_k (1 - \xi_{p^r}^k) = p$, *onde o produto é tomado sobre os* k, *com* $1 \leq k \leq p^r$, *e tal que* $p \nmid k$.

Demonstração. Como $\phi_{p^r}(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + ... + x^{(p-1)p^{r-1}}$, segue que todos os $\xi_{p^r}^k$, onde $1 \leq k \leq p^r$ e tal que $p \nmid k$ são raízes de $\phi_{p^r}(x)$ pois são raízes de $x^{p^r} - 1$ mas não de $x^{p^{r-1}} - 1$. Deste modo, $\phi_{p^r}(x) = \prod_k (x - \xi_{p^r}^k)$ e existem exatamente $\phi(p^r) = (p-1)p^{r-1}$ valores de k pois $\partial(\phi_{p^r}(x)) = (p-1)p^{r-1}$. Tomando $x = 1$, temos que $\phi_{p^r}(1) = \prod_k (1 - \xi_{p^r}^k) = 1 + 1^{p^{r-1}} + ... + 1^{(p-1)p^{r-1}} = p$. □

Os próximos resultados que vamos enunciar serão usados na demonstração do Teorema 3.5.

Lema 3.3. *(Lema de Gauss) Se* $f(x) \in \mathbb{Z}[x]$, *e*

$$f(x) = g(x)h(x) \text{ para } g(x), h(x) \in \mathbb{Q}[x],$$

então

$$f(x) = G(x)H(x) \text{ para alguns } G(x), H(x) \in \mathbb{Z}[x].$$

Além disso, $\partial_{\mathbb{Q}}(g) = \partial_{\mathbb{Z}}(G)$, *e* $\partial_{\mathbb{Q}}(h) = \partial_{\mathbb{Z}}(H)$.

Teorema 3.4. *(Pequeno Teorema de Fermat) Se p é primo e $a \in \mathbb{Z}$, então*

$$a^p \equiv a(mod\ p).$$

Em particular, se $p \nmid a$, então

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

Teorema 3.5. *[6] Se ζ_n é uma raiz n-ésima primitiva da unidade, então $[\mathbb{Q}(\zeta_n) : \mathbb{Q})] = \phi(n)$.*

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

Como consequência do pequeno Teorema de Fermat, temos que $a^p \equiv a(mod\ p)$ e daí $h(x^p) \equiv h(x)^p(mod\ p)$. Assim, $f(x)g(x) \equiv h(x)^p(mod\ p)$, e portanto $h(x)^p \equiv f(x)g(x)(mod\ p)$. Logo, $\overline{h(\xi_n)^p} = \overline{0}$, pois ξ_n é raiz de $f(x)$. E recursivamente chegamos que $\overline{h}(\xi_n) = 0$.

Portanto $\overline{f}$ e $\overline{h}$ tem uma raiz em comum. Assim $x^n - \overline{1} = \overline{f}(x)\overline{g}(x)$, e portanto $x^n - \overline{1}$ tem raízes múltiplas. Logo $nx^{n-1} = \overline{0}$ e assim, para qualquer $\alpha \in \mathbb{Z}_p, n\alpha^{n-1} = \overline{0}$. Como a característica de $\mathbb{Z}_p$ é p segue que $p|n$, o que contradiz o fato de termos suposto que $p \nmid n$. Portanto ξ_n^p é a raiz de $f(x)\ \forall\ p \nmid n$ e $mdc(p, n) = 1$. Logo $\partial(f(x)) \geq \partial(\phi_n(x))$, pois toda raiz de $\phi_n(x)$ é raiz de $f(x)$, e como $f(x)|\phi_n(x)$, segue que $\partial(\phi_n(x)) \geq \partial(f(x))$. Portanto $\partial(f(x)) = \partial(\phi_n(x)) = \phi(n)$. □

Teorema 3.6. *[17] Se ζ_n é uma raiz n-ésima primitiva da unidade, então o anel dos inteiros de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{Z}$ é $\mathbb{Z}[\zeta_n]$ e uma $\mathbb{Z} - base$ de $\mathbb{Z}[\zeta_n]$ é $\{1, \zeta_n, ..., \zeta_n^{\phi(n)-1}\}$.*

Proposição 3.4. *[17] Os $\mathbb{Q}$-monomorfismos de $\mathbb{Q}(\zeta_n)$ sobre $\mathbb{C}$ são dados por $\{\sigma_i, mdc(i, n) = 1, i = 1, ..., n-1, \sigma_i(\zeta) = \zeta^i\}$.*

Proposição 3.5. *Se p é um número primo ímpar e $\zeta = \zeta_{p^r}$ uma raiz p^r-ésima primitiva da unidade, com r um inteiro positivo, então o discriminante de $\mathbb{Q}(\zeta_{p^r})$ sobre $\mathbb{Q}$ satisfaz*

$$\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, ..., \zeta_{p^r}^{\phi(p^r)-1}) = \pm p^{p^{r-1}(r(p-1)-1)}$$

.

Demonstração. Pela Proposição 2.3, temos que

$$\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, ..., \zeta_{p^r}^{\phi(p^r)-1}) = \pm N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(f'(\zeta_{p^r})).$$

Derivando ambos os lados de $f(x) = \dfrac{x^{p^r}-1}{x^{p^{r-1}}-1}$, temos que

$$f'(x) = \frac{p^r x^{p^{r-1}}(x^{p^{r-1}}-1) - (x^{p^r}-1)p^{r-1}x^{p^{r-1}-1}}{(x^{p^{r-1}}-1)^2}, \tag{3.3}$$

e substituindo x por ζ_{p^r} na equação 3.3, temos que

$$f'(\zeta_{p^r}) = \frac{p^r \zeta_{p^r}^{p^r-1}(\zeta_{p^r}^{p^{r-1}}-1) - (\zeta_{p^r}^{p^r}-1)p^{r-1}\zeta_{p^r}^{p^{r-1}-1}}{(\zeta_{p^r}^{p^{r-1}}-1)^2}$$

Como $\zeta_{p^r}^{p^r} = 1$, segue que $f'_{p^r}(\zeta_{p^r}) = \frac{p^r\zeta_{p^r}^{-1}}{\zeta_{p^r}^{p^{r-1}}-1} = \frac{-p^r}{(1-\zeta_{p^r}^{p^{r-1}})\zeta_{p^r}}$, pois $\zeta_{p^r}^{p^{r-1}} = (e^{\frac{2\pi i}{p^r}})^{p^{r-1}} = e^{\frac{2\pi i}{p}} = \zeta_p$. Aplicando a função norma em ambos os membros e usando sua linearidade, temos que

$$N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(f'(\zeta_{p^r})) = \frac{N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(-p^r)}{N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1-\zeta_p)N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r})}.$$

Temos que $N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}) = \pm 1$. Também, $N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(-p^r) = (-p^r)^{(p-1)p^{r-1}}$ e $N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1-\zeta_p) = N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}(\zeta_p)}(1-\zeta_p) = (N_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1-\zeta_p))^{p^{r-1}} = p^{p^{r-1}}$.

Portanto, $\mathcal{D}_{\mathbb{K}|\mathbb{Q}}(1, \zeta_{p^r}, ..., \zeta_{p^r}^{\phi(p^r)-1}) = \frac{\pm p^{r(p-1)p^{r-1}}}{p^{p^{r-1}}} = \pm p^{p^{r-1}(r(p-1)-1)}$. □

Como consequência da Proposição 3.4 segue que

- se $n = p$, então $\mathcal{D}_{\mathbb{L}/\mathbb{Q}} = (-1)^{\frac{(p-1)}{2}}p^{p-2}$;
- se $n = p^r$, então $\mathcal{D}_{\mathbb{L}/\mathbb{Q}} = (-1)^{\frac{(p-1)p^{r-1}}{2}}p^{p^{r-1}\cdot(r(p-1)-1)}$, r inteiro positivo.

O subcorpo real maximal dos corpos ciclotômicos é muito utilizado por suas propriedades e será definido a seguir.

Proposição 3.6. *[17] Se $n \in \mathbb{N}^*$, ζ_n é uma raiz n-ésima primitiva da unidade e $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, então $\mathbb{K}$ é totalmente real e $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = 2$.*

Demonstração. Seja $f(x) = x^2 - (\zeta_n + \zeta_n^{-1})x + 1 \in \mathbb{K}[x]$. Temos que $f(\zeta_n) = 0$. Além disso, como ζ_n não pertence $\mathbb{K}$, segue que f é irredutível sobre $\mathbb{K}$. Logo, $f = min_{\mathbb{K}}\zeta_n$. Desta forma, $[\mathbb{Q}(\zeta_n) : \mathbb{K}] = \partial(f) = 2$. □

Definição 3.6. *Nas condições da proposição acima, o corpo $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é chamado de* ***subcorpo real maximal*** *de $\mathbb{Q}(\zeta_n)$.*

Teorema 3.7. *[17] O anel dos inteiros de $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ é $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ e uma $\mathbb{Z}$-base de $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ é*

$$\{1, \zeta_n + \zeta_n^{-1}, \zeta_n^2 + \zeta_n^{-2}, ..., \zeta_n^{\frac{\phi(n)}{2}-1} + \zeta_n^{\frac{\phi(n)}{2}+1}\}.$$

Teorema 3.8. *[17] O discriminante de* $\mathbb{K} = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ *sobre* $\mathbb{Q}$ *é dado por:*

- $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = p^{\frac{p-3}{2}}$, *se* $n = p \geq 5$;
- $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = 2^{(r-1)2^{r-2}-1}$, *se* $n = 2^r$;
- $\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = p^{\frac{(r+1)(p-1)p^{r-1}-p^r-1}{2}}$, *se* $n = p^r, p \neq 2, r > 1$.

4 Ideais e Norma de um Ideal

Neste capítulo, vamos definir ideais para a introdução de dois tipos de domínios com base na teoria de ideais que tem influência em fatoração de ideais e em teoria dos números algébricos. A norma de um ideal nos será útil para o cálculo do volume de reticulados, assunto que será visto no Capítulo 5.

As principais referências utilizadas foram [8], [11] e [15].

4.1 Ideais

Nesta seção apresentamos os conceitos e algumas propriedades de ideais.

Definição 4.1. *Um R-**ideal** I é um subconjunto não vazio de um anel comutativo R com identidade e com as seguintes propriedades*

(a) Se $\alpha, \beta \in I$, então $\alpha + \beta \in I$.

(b) Se $\alpha \in I$ e $r \in R$, então $r\alpha \in I$.

Definição 4.2. *Um domínio A é dito um **corpo** se cada elemento diferente de zero é uma unidade.*

Observação 4.1. Indutivamente, a Definição 4.1 implica que se $\alpha_1, \alpha_2, ..., \alpha_n \in I$ para qualquer $n \in \mathbb{N}$, então $r_1\alpha_1 + r_2\alpha_2 + ... + r_n\alpha_n \in I$ para qualquer $r_1, r_2, ..., r_n \in R$. Se $1 \in I$, então $I = R$. Se nos é dado um conjunto de elementos $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ em um domínio R, então o conjunto de todas as combinações lineares de α_j para $j = 1, 2, ..., n$

$$\left\{ \sum_{j=1}^{n} r_j\alpha_j : r_j \in R \text{ para } j = 1, 2, ..., n \right\}$$

é um ideal de R denotado por $\langle \alpha_1, \alpha_2, ..., \alpha_n \rangle$.

Em particular, quando $n = 1$, temos a seguinte definição:

Definição 4.3. *Se A é um domínio e I é um A-ideal, então I é chamado de A-ideal **principal** se existe um elemento $\alpha \in I$ tal que $I = \langle \alpha \rangle$, onde α é chamado de **gerador** de I. Se $I \neq A$, então I é chamado de ideal **próprio**.*

Exemplo 4.1. Seja $n \in \mathbb{Z}$ e seja $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, um ideal em $\mathbb{Z}$. Temos que $n\mathbb{Z} = \langle n \rangle = \langle -n \rangle$ é de fato um ideal principal e é um ideal próprio para todo $n \neq \pm 1$.

Exemplo 4.2. Em $A = \mathbb{Z}[i]$, temos que $2\mathbb{Z}[i]$ e $3\mathbb{Z}[i]$ são ideais principais próprios.

Definição 4.4. *Se A é um domínio, então o A-ideal próprio $\mathcal{P}$ é chamado de **A-ideal primo** se satisfaz a propriedade que, sempre que $\alpha\beta \in \mathcal{P}$, para $\alpha, \beta \in A$, ou então $\alpha \in \mathcal{P}$ ou $\beta \in \mathcal{P}$.*

Definição 4.5. *Sejam I, J ideais primos de $\mathcal{O}_{\mathbb{L}}$. Dizemos que I e J são **ideais primos conjugados** de $\mathcal{O}_{\mathbb{L}}$ se existe $\sigma \in G = Gal(\mathbb{L}/\mathbb{K})$ tal que $\sigma(I) = J$.*

A fim de discutir quaisquer mais recursos da teoria de ideal, precisamos entender como é feita a multiplicação de ideais.

Definição 4.6. *Se A é um domínio e I, J são A-ideais, então o **produto** de I e J, denotado por IJ, é o ideal em A dado por*

$$IJ = \{r \in A : r = \sum_{j=1}^{n} \alpha_j \beta_j \text{ onde } n \in \mathbb{N}, \text{ e } \alpha_j \in I, \beta_j \in J \text{ para } 1 \leq j \leq n\}.$$

Definição 4.7. *Em um domínio A, um ideal M é chamado **maximal** se satisfaz a propriedade que, sempre que $M \subseteq I \subseteq A$, para qualquer A-ideal I, então $I = A$ ou $I = M$.*

Teorema 4.1. *[1] Seja A um domínio e sejam $a, b \in A^* = A \setminus \{0\}$. Então*

$\langle a \rangle = \langle b \rangle$ se, e somente se, a/b pertence ao conjunto das unidades de A, isto é, $(a/b) \,|1$.

Demonstração. Se a/b pertence ao conjunto das unidades de A então $a = bu$ para qualquer u pertencente ao conjunto das unidades de A. Seja $x \in \langle a \rangle$. Então $x = ac$ para algum $c \in A$. Assim, $x = buc$ com $uc \in D$. Logo $x \in \langle b \rangle$.

Mostramos que $\langle a \rangle \subseteq \langle b \rangle$. Como a/b pertence ao conjunto das unidades de A e esse conjunto é um grupo multiplicativo, temos $b/a = (a/b)^{-1}$ pertencente ao conjunto de unidades de A. Então, procedendo como antes, com as funções de a e b trocados, descobrimos que $\langle b \rangle \subseteq \langle a \rangle$. Portanto $\langle a \rangle = \langle b \rangle$.

Por outro lado, suponha que $\langle a \rangle = \langle b \rangle$. Então $a = bc$ para algum $c \in A$ e $b = ad$ para algum $d \in A$. Assim $b = bcd$, como $b \neq 0$ deduzimos que $1 = cd$ de modo que c pertence ao conjunto de unidades de A. Portanto $a/b = c$ que pertence ao conjunto de unidades de A. □

4.2 Norma de um Ideal

Nesta seção veremos o Teorema da fatoração única de ideais e norma de ideais. Para isto, sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_{\mathbb{K}}$ o anel de inteiros de $\mathbb{K}$.

Definição 4.8. *Seja I um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. A* ***norma*** *de I é definida como a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}/I$, isto é,*

$$N(I) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right).$$

Proposição 4.1. *[11] Se $\alpha \in \mathcal{O}_{\mathbb{K}}$; $\alpha \neq 0$ e $I = \alpha\mathcal{O}_{\mathbb{K}}$ é um ideal de $\mathcal{O}_{\mathbb{K}}$, então $N(I) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = |N_{\mathbb{K}|\mathbb{Q}}(\alpha)|$.*

Exemplo 4.3. Se $\mathbb{F} = \mathbb{Q}(\sqrt{d})$ e $\alpha = (a + b\sqrt{d})/2 \in \mathcal{O}_{\mathbb{F}}$ sendo d um inteiro livre de quadrados, então

$$N(\langle\alpha\rangle) = |N_{\mathbb{F}}(\alpha)| = \frac{a^2 - b^2 d}{4}.$$

O próximo teorema será usado na demonstração de alguns resultados desta seção.

Teorema 4.2. *(Teorema do Isomorfismo) Se R e S são anéis comutativos com identidade e*

$$\phi : R \to S$$

é um homomorfismo de anéis, então

$$R/Ker(\phi) \cong Im(\phi).$$

Proposição 4.2. *Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então $N(I)$ é finita.*

Demonstração. Se $\alpha \in I$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset I$. Consideremos a aplicação

$$\begin{aligned} \phi : \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) &\longrightarrow \left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right) \\ x + \mathcal{O}_{\mathbb{K}}\alpha &\longmapsto x + I \end{aligned}$$

Temos que ϕ é um homomorfismo sobrejetor e $Ker(\phi) = \left(\frac{I}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$. De fato, $x + \mathcal{O}_{\mathbb{K}}\alpha \in Ker(\phi)$ se, e somente se, $\phi(x + \mathcal{O}_{\mathbb{K}}\alpha) = x + I = 0$ se, e somente se, $x \in I$. Desta forma, pelo Teorema do Isomorfismo, segue que

$$\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) \Big/ \left(\frac{I}{\mathcal{O}_{\mathbb{K}}\alpha}\right) \simeq \left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right).$$

Assim, segue que

$$\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right)\#\left(\frac{I}{\mathcal{O}_{\mathbb{K}}\alpha}\right).$$

Pela Proposição 4.1, temos que $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)$ é finito. Portanto, $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right)$ é finito. □

Definição 4.9. *Um domínio é dito de Dedekind se for integralmente fechado, Noetheriano (seus ideais são finitamente gerados) e se todo ideal primo não nulo for maximal.*

Exemplo 4.4. $\mathcal{O}_{\mathbb{K}}$, o anel dos inteiros de um corpo de números $\mathbb{K}$, é um anel de Dedekind. ([1], pg. 194)

Teorema 4.3. *[8] (Fatoração única de ideais) Todo ideal próprio não-nulo em um domínio de Dedekind D é representado unicamente como um produto de ideais primos. Em outras palavras, qualquer D-ideal tem uma representação única de forma que*

$$I = \mathcal{P}_1^{a_1} \cdot \mathcal{P}_2^{a_2} \cdots \mathcal{P}^{a_n},$$

onde os $\mathcal{P}_j$ são os D-ideais primos distintos contendo I, e $a_j \in \mathbb{N}$ para $j = 1, 2, ..., n$.

Definição 4.10. *Suponha que A é um domínio com corpo de fração $\mathbb{F}$. Então um subconjunto não vazio I de $\mathbb{F}$ é chamado de A-ideal* ***fracionário*** *se satisfaz as três propriedades:*

1. $\forall\ \alpha, \beta \in I, \alpha + \beta \in I.$
2. $\forall\ \alpha \in I \ e\ r \in A, r\alpha \in I.$
3. $\exists\ \gamma \in D\ com\ \gamma \neq 0\ tal\ que\ \gamma I \subseteq A.$

Observação 4.2. Todo ideal de A é também um ideal fracionário, basta tomar $\gamma = 1$.

Os resultados que seguem serão usadas na demonstração da Proposição 4.4.

Definição 4.11. *Suponha que M é um grupo abeliano aditivo e que R é um anel. Segue que um subconjunto N de M é um R-**submódulo** de M se, e somente se*

(a) $0 \in N;$

(b) $\forall\ m, n \in N, m - n \in N;$

(c) $\forall\ r \in R\ e\ n \in N, rn \in N.$

Observação 4.3. Para a definição de **módulo** consultar [[15],pg 25].

Proposição 4.3. *[11] Se A é um anel de Dedekind que não é corpo, então todo ideal fracionário é inversível.*

Para a demonstração da Proposição a seguir vamos usar o conceito de anel de Dedekind. Este conceito também será muito utilizado no Capítulo 6.

Proposição 4.4. *Se I e J são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $N(IJ) = N(I)N(J)$.*

Demonstração. Como $\mathcal{O}_{\mathbb{K}}$ é um anel de Dedekind e J é um ideal de $\mathcal{O}_{\mathbb{K}}$, pelo Teorema 4.3, segue que $J = \prod_{i=1}^{n} \mathcal{P}_i^{e_i}$, onde os $\mathcal{P}_i's$ são ideais primos não nulos de $\mathcal{O}_{\mathbb{K}}$ e $e_i \geq 0$, $i = 1, ..., n$. Além disso, como $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind, segue que os ideais $\mathcal{P}_i's$ são maximais. Seja $\mathcal{P}_i = M$, para algum $i = 1, ..., n$. Por indução sobre o número de

fatores é suficiente provar que $N(IM) = N(I)N(M)$. Segue, da definição de norma de ideal, que a igualdade anterior se verifica se, e somente se,

$$\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{IM}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right)\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{M}\right).$$

Temos que o homomorfismo $\phi : \frac{\mathcal{O}_{\mathbb{K}}}{IM} \longrightarrow \frac{\mathcal{O}_{\mathbb{K}}}{I}$, definido por $\phi(x+IM) = x+I$, é sobrejetor e $Ker(\phi) = \frac{I}{IM}$. Assim, pelo Teorema do Isomorfismo, temos que $\left(\frac{\mathcal{O}_{\mathbb{K}}}{IM}\right) \diagup \left(\frac{I}{IM}\right) \simeq \left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right)$ Logo,

$$\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{IM}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right)\#\left(\frac{I}{IM}\right).$$

Podemos, então, concluir que $N(IM) = N(I)N(M)$ se verifica se, e somente se, $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{M}\right) = \#\left(\frac{I}{IM}\right)$. Agora, temos que $\frac{I}{IM}$ é um espaço vetorial sobre $\frac{\mathcal{O}_{\mathbb{K}}}{M}$ mediante as operações:

$$\begin{array}{rcl} +: \dfrac{I}{IM} \times \dfrac{I}{IM} & \longrightarrow & \dfrac{I}{IM} \\ (x+IM, y+IM) & \longmapsto & (x+y)+IM \end{array}$$

$$\begin{array}{rcl} \cdot: \dfrac{\mathcal{O}_{\mathbb{K}}}{M} \times \dfrac{I}{IM} & \longrightarrow & \dfrac{I}{IM} \\ (\alpha+M, x+IM) & \longmapsto & (\alpha x)+IM. \end{array}$$

Além disso, temos que os $\frac{\mathcal{O}_{\mathbb{K}}}{M}$-submódulos de $\frac{I}{IM}$ são ideais e são do tipo $\frac{B}{IM}$, onde B é um ideal tal que $IM \subseteq B \subseteq I$. Mas, como todo ideal num domínio de Dedekind admite inverso, segue que $I^{-1}IM \subseteq I^{-1}B \subseteq I^{-1}I$, ou seja, $M \subseteq I^{-1}B \subseteq \mathcal{O}_{\mathbb{K}}$. Como M é maximal, segue que $M = I^{-1}B$ ou $I^{-1}B = \mathcal{O}_{\mathbb{K}}$. Assim, $IM = B$ ou $B = I$. Portanto, não existe B tal que $IM \subsetneq B \subsetneq I$. Assim, os $\frac{\mathcal{O}_{\mathbb{K}}}{M}$-submódulos de $\frac{I}{IM}$, ou os subespaços do espaço vetorial $\frac{I}{IM}$, são apenas os triviais. Portanto, $dim_{\frac{\mathcal{O}_{\mathbb{K}}}{M}} \frac{I}{IM} = 1$ e, deste modo, $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{M}\right) = \#\left(\frac{I}{IM}\right)$, o que implica que $N(IM) = N(I)N(M)$. □

Proposição 4.5. *Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então:*

1. *$N(I) = 1$ se, e somente se, $I = \mathcal{O}_{\mathbb{K}}$.*
2. *Se $N(I)$ for um número primo então o ideal I é primo.*

Demonstração.

1. Temos que $N(I) = 1$ se, e somente se, $\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right) = 1$ se, e somente se, $I = \mathcal{O}_{\mathbb{K}}$.
2. Suponhamos que I não seja um ideal primo. Assim, $I = \mathcal{O}_{\mathbb{K}}$ ou $I = \mathcal{Q}_1\mathcal{Q}_2$, onde $\mathcal{Q}_1$, $\mathcal{Q}_2$ são ideais não nulos distintos de $\mathcal{O}_{\mathbb{K}}$. Se $I = \mathcal{O}_{\mathbb{K}}$, pelo item (1), temos que $N(I) = 1$, o que é contra a hipótese. Se $I = \mathcal{Q}_1\mathcal{Q}_2$ temos, pela Proposição 4.4, que $N(I) = N(\mathcal{Q}_1)N(\mathcal{Q}_2)$ e, como por hipótese, $N(I) = p$, p primo, segue que $N(\mathcal{Q}_1) = 1$ e $N(\mathcal{Q}_2) = p$ ou $N(\mathcal{Q}_1) = p$ e $N(\mathcal{Q}_2) = 1$. Logo, $\mathcal{Q}_1 = \mathcal{O}_{\mathbb{K}}$ ou $\mathcal{Q}_2 = \mathcal{O}_{\mathbb{K}}$, o que é contra a hipótese. Portanto, I é um ideal primo de $\mathcal{O}_{\mathbb{K}}$. □

Proposição 4.6. *[15] Se I é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$ tal que $\{w_1, ..., w_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ e $\{y_1, ..., y_n\}$ é uma $\mathbb{Z}$-base de I, com $y_i = \sum_{j=1}^{n} a_{ij} w_j$, $i = 1, \cdots, n$, então $N(I) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{I}\right) = det(a_{ij})$.*

Teorema 4.4. *[8] Suponha que $\mathbb{F}$ é um corpo de números, e que I é um ideal diferente de zero de $\mathcal{O}_{\mathbb{F}}$. Se $\mathcal{B} = \{\alpha_1, ..., \alpha_n\}$ é uma $\mathbb{Z}$-base para I, então*

$$N(I)^2 = \frac{\mathcal{D}(\mathcal{B})}{\mathcal{D}_{\mathbb{F}}}.$$

onde $\mathcal{D}_{\mathbb{F}}$ é o discriminante de $\mathbb{F}$.

Demonstração. Seja $\mathcal{B}_1 = \{\beta_1, ..., \beta_n\}$ uma $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{F}}$. Então para cada $i = 1, .., n$

$$\alpha_i = \sum_{j=1}^{n} z_{i,j}\beta_j, \qquad (z_{i,j} \in \mathbb{Z}).$$

Pela Proposição 4.6,

$$N(I) = |\mathcal{O}_{\mathbb{F}}/I| = |det(z_{i,j})|.$$

Pelo Teorema 2.6,

$$\mathcal{D}(\mathcal{B}) = (det(z_{i,j}))^2 \mathcal{D}(\mathcal{B}_1) = N(I)^2 \mathcal{D}_{\mathbb{F}},$$

como queríamos. □

4.3 Decomposição em Ideais Primos

Seja $\mathbb{K}$ um corpo de números e seja $\mathcal{P}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$, o anel dos inteiros de $\mathbb{K}$. Então $\mathcal{P} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$. [11]

Uma vez que $\mathcal{P} \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$, deve existir um número primo p tal que $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$. Dizemos então que $\mathcal{P}$ **está acima** de p.

Podemos visualizar da seguinte forma:

$$\begin{array}{c} \mathcal{P} \subset \mathcal{O}_{\mathbb{K}} \subset \mathbb{K} \\ | \\ p\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \end{array}$$

Chamamos de **corpo de resíduos** o quociente de um anel comutativo por um ideal maximal. Assim, o corpo de resíduos $\mathbb{Z}/p\mathbb{Z}$ é $\mathbb{F}_p$. Estamos interessados no corpo de resíduos $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$. Vamos mostrar que $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$ é um $\mathbb{F}_p$-espaço vetorial de dimensão finita. Considere a composição

$$\mathbb{Z} \xrightarrow{\iota} \mathcal{O}_{\mathbb{K}} \xrightarrow{\pi} \mathcal{O}_{\mathbb{K}}/\mathcal{P},$$

onde a primeira seta é a inclusão canônica ι de $\mathbb{Z}$ em $\mathcal{O}_{\mathbb{K}}$, e a segunda seta é a projeção π. Denotamos $\phi : \pi \circ \iota$. Segue que, o kernel de ϕ é dado por

$$ker(\phi) = \{a \in \mathbb{Z} | a \in \mathcal{P}\} = \mathcal{P} \cap \mathbb{Z} = p\mathbb{Z},$$

de modo que ϕ induz uma injeção de $\mathbb{Z}/p\mathbb{Z}$ em $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$, pois $\mathbb{Z}/p\mathbb{Z} \simeq Im(\phi) \subset \mathcal{O}_{\mathbb{K}}/\mathcal{P}$. Pela Proposição 4.2, $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$ é um conjunto finito, portanto, um corpo finito que contém $\mathbb{Z}/p\mathbb{Z}$ e temos, de fato, uma extensão finita de $\mathbb{F}_p$.

Definição 4.12. *Chamamos de* ***grau de inércia****, e denotamos por $f_{\mathcal{P}}$, a dimensão do $\mathbb{F}_p$-espaço vetorial $\mathcal{O}_{\mathbb{K}}/\mathcal{P}$, isto é*

$$f_{\mathfrak{p}} = dim_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{K}}/\mathcal{P}).$$

Em particular,

$$N(\mathcal{P}) = |\mathcal{O}_{\mathbb{K}}/\mathcal{P}| = |\mathbb{F}_p^{dim_{\mathbb{F}_p}(\mathcal{O}_{\mathbb{K}}/\mathcal{P})}| = |\mathbb{F}_p|^{f_{\mathcal{P}}} = p^{f_{\mathcal{P}}}.$$

Exemplo 4.5. Considere o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$, com anel dos inteiros $\mathbb{Z}[i]$, e seja o ideal $2\mathbb{Z}[i]$:

$$2\mathbb{Z}[i] = (1+i)(1-i)\mathbb{Z}[i] = \mathcal{P}^2, \ \mathcal{P} = (1+i)\mathbb{Z}[i] = (1-i)\mathbb{Z}[i]$$

pois $(-i)(1+i) = 1-i$. Além disso, $\mathcal{P} \cap \mathbb{Z} = 2\mathbb{Z}$, de modo que $\mathcal{P} = \langle 1+i \rangle$ é dito estar acima de 2. Temos que

$$N(\mathcal{P}) = N_{\mathbb{K}/\mathbb{Q}}(\langle 1+i \rangle) = (1+i)(1-i) = 2$$

e assim $f_{\mathcal{P}} = 1$. De fato, o corpo de resíduo correspondente é

$$\mathcal{O}_{\mathbb{K}}/\mathcal{P} \simeq \mathbb{F}_2.$$

Definição 4.13. *Seja $p \in \mathbb{Z}$ um primo. Seja $\mathcal{P}$ um ideal primo de $\mathcal{O}_{\mathbb{K}}$ acima de p. Chamamos de* ***índice de ramificação*** *de $\mathcal{P}$, e denotamos $e_{\mathcal{P}}$, a potência exata de $\mathcal{P}$ que divide $p\mathcal{O}_{\mathbb{K}}$.*

Seja $p \in \mathbb{Z}$, cuja fatoração em $\mathcal{O}_{\mathbb{K}}$ é dada por

$$p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1^{e_{\mathcal{P}_1}} \cdots \mathcal{P}_g^{e_{\mathcal{P}_g}}.$$

Dizemos que p é ***ramificado*** *se $e_{\mathcal{P}_i} > 1$ para algum i. Caso contrário, se*

$$p\mathcal{O}_{\mathbb{K}} = \mathcal{P}_1 \cdots \mathcal{P}_g, \quad \mathcal{P}_i \neq \mathcal{P}_j, \quad i \neq j,$$

p é ***não-ramificado***.

Tanto o grau de inércia e o índice de ramificação são ligados através do grau do corpo de números da seguinte forma:

Proposição 4.7. *[11] Sejam $\mathbb{K}$ um corpo de números de grau n e $\mathcal{O}_\mathbb{K}$ o anel de inteiros de $\mathbb{K}$. Seja $p \in \mathbb{Z}$ e seja*

$$p\mathcal{O}_\mathbb{K} = \mathcal{P}_1^{e_{\mathcal{P}_1}} \cdots \mathcal{P}_g^{e_{\mathcal{P}_g}}$$

sua fatoração em $\mathcal{O}_\mathbb{K}$. Temos que

$$n = [\mathbb{K} : \mathbb{Q}] = \sum_{i=1}^{g} e_{\mathcal{P}_i} f_{\mathcal{P}_i}.$$

Observação 4.4. Em geral, não existe método simples para calcular a fatoração de $p\mathcal{O}_\mathbb{K}$. No entanto, no caso em que o anel de inteiros $\mathcal{O}_\mathbb{K}$ é da forma $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$, podemos usar o seguinte resultado.

Proposição 4.8. *Sejam $\mathbb{K}$ um corpo de números, com anel de inteiros $\mathcal{O}_\mathbb{K}$ e p um primo. Vamos supor que existe θ tal que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$, e seja f o polinômio minimal de θ, cuja redução módulo p é denotada por $\overline{f}$. Considere*

$$\overline{f}(x) = \prod_{i=1}^{g} \overline{\phi_i}(x)^{e_i}$$

a fatoração de $f(x)$ em $\mathbb{F}_p[x]$, com $mdc(\phi_i(x), \phi_j(x)) = 1$, $i \neq j$ e irredutível. Temos

$$\mathcal{P}_i = \langle p, f_i(\theta) \rangle = p\mathcal{O}_\mathbb{K} + f_i(\theta)\mathcal{O}_\mathbb{K}$$

onde $\overline{f}_i = \overline{\phi_i}(mod\ p)$, então

$$p\mathcal{O}_\mathbb{K} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}$$

é a fatoração de $p\mathcal{O}_\mathbb{K}$ em $\mathcal{O}_\mathbb{K}$.

A proposição acima dá um método concreto para calcular a fatoração de um primo $p\mathcal{O}_\mathbb{K}$, a saber:

1. Escolha um primo $p \in \mathbb{Z}$ cuja fatoração em $p\mathcal{O}_\mathbb{K}$ deve ser calculada.
2. Seja f o polinômio minimal de θ tal que $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\theta]$.
3. Calcule a fatoração de $\overline{f} \equiv f(mod\ p)$:

$$\overline{f} = \prod_{i=1}^{g} \overline{\phi_i}(x)^{e_i}.$$

4. Levante cada $\overline{\phi_i}$ a um polinômio $f_i \in \mathbb{Z}[x]$.

5. Calcule $\mathfrak{p} = \langle p, f_i(\theta)\rangle$ avaliando f_i em θ.

6. A fatoração de $p\mathcal{O}_\mathbb{K}$ é dada por

$$p\mathcal{O}_\mathbb{K} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_g^{e_g}.$$

Exemplo 4.6. 1. Consideremos $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$, com anel de inteiros $\mathcal{O}_\mathbb{K} = \mathbb{Z}[\sqrt[3]{2}]$. Queremos a fatorar $5\mathcal{O}_\mathbb{K}$. Pela proposição acima, calculamos

$$x^3 - 2 = (x-3)(x^2+3x+4) \equiv (x+2)(x^2-2x-1)(mod\ 5).$$

Assim, obtemos que

$$5\mathcal{O}_\mathbb{K} = \mathcal{P}_1\mathcal{P}_2,\ \mathcal{P}_1 = \langle 5, 2+\sqrt[3]{2}\rangle,\ \mathcal{P}_2 = \langle 5, \sqrt[3]{4} - 2\sqrt[3]{2} - 1\rangle.$$

2. Consideremos $\mathbb{Q}(i)$, com $\mathcal{O}_\mathbb{K} = \mathbb{Z}[i]$, e escolhemos $p = 2$. Temos $\theta = i$ e $f(x) = x^2 + 1$. Calculamos a fatoração de $\overline{f}(x) = f(x)(mod\ 2)$:

$$x^2 + 1 \equiv x^2 - 1 \equiv (x-1)(x+1) \equiv (x-1)^2(mod\ 2).$$

Podemos tomar qualquer levantamento dos fatores em $\mathbb{Z}[x]$, e assim podemos escrever

$$2\mathcal{O}_\mathbb{K} = \langle 2, i-1\rangle\langle 2, i+1\rangle \text{ ou } 2 = \langle 2, i-1\rangle^2$$

que é a mesma, pois que $\langle 2, i-1\rangle = \langle 2, i+1\rangle$. Além disso, como $2 = (1-i)(1+i)$, vemos que $\langle 2, i-1\rangle = \langle 1+i\rangle$, que é o resultado do Exemplo 4.5.

Definição 4.14. *Dizemos que p é **inerte** se $p\mathcal{O}_\mathbb{K}$ é primo, e neste caso temos que $g = 1$, $e = 1$ e $f = n$. Dizemos que p é **totalmente ramificado** se $e = n$, $g = 1$ e $f = 1$.*

O discriminante de $\mathbb{K}$ nos dá informações sobre a ramificação em $\mathbb{K}$.

Teorema 4.5. *[11] Seja $\mathbb{K}$ um corpo de números. Então p é ramificado se, e somente se, p divide o discriminante $\mathcal{D}_\mathbb{K}$.*

Exemplo 4.7. No Exemplo 4.5, vimos que 2 ramifica em $\mathbb{K} = \mathbb{Q}(i)$. Então 2 deve aparecer em $\mathcal{D}_\mathbb{K}$. Pode-se verificar que $\mathcal{D}_\mathbb{K} = -4$.

A definição que segue será usada na Definição 4.16.

Definição 4.15. *(Símbolo de Kronecker) Suponha que $n \in \mathbb{N}$ e $\mathcal{D}_{\mathbb{F}}$ é o discriminante de um corpo de números quadráticos.*

O ***símbolo de Kronecker*** $\left(\frac{\mathcal{D}_{\mathbb{F}}}{n}\right)$ *é dado por*

$$\left(\frac{\mathcal{D}_{\mathbb{F}}}{n}\right) = 0$$

se $mdc(\mathcal{D}_{\mathbb{F}}, n) > 1$, *e*

$$\left(\frac{\mathcal{D}_{\mathbb{F}}}{2}\right) = \begin{cases} 1 \text{ se } \mathcal{D}_{\mathbb{F}} \equiv 1 \ (mod\ 8), \\ -1 \text{ se } \mathcal{D}_{\mathbb{F}} \equiv 5 \ (mod\ 8). \end{cases}$$

$\left(\frac{\mathcal{D}_{\mathbb{F}}}{p}\right)$ *é o símbolo de Legendre para qualquer primo* $p > 2$.

$\left(\frac{\mathcal{D}_{\mathbb{F}}}{n}\right)$ *é o símbolo de Jacobi se* n *é ímpar e* $mdc(n, \mathcal{D}_{\mathbb{F}}) = 1$.

Se $n = 2^a m$ *onde* m *é ímpar, então*

$$\left(\frac{\mathcal{D}_{\mathbb{F}}}{n}\right) = \left(\frac{\mathcal{D}_{\mathbb{F}}}{2}\right)^a \left(\frac{\mathcal{D}_{\mathbb{F}}}{m}\right),$$

onde $\left(\frac{\mathcal{D}_{\mathbb{F}}}{m}\right)$ *é o símbolo de Jacobi.*

Definição 4.16. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, d *um inteiro livre de quadrados,* p *um primo em* $\mathbb{Z}$ *e* $p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{m} \mathcal{Q}_i^{e_i}$. *Seguem as afirmações:*

(i) Se $m = 2, e_1 = e_2 = 1, f(\mathcal{Q}_i|P) = 1$, *então* $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1\mathcal{Q}_2, \mathcal{Q}_1 \neq \mathcal{Q}_2$. *Dizemos que* p *se fatora em* $\mathbb{K}$.

(ii) Se $m = 1, e_1 = 2, f(\mathcal{Q}_1|P) = 1$, *então* $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1^2$. *Dizemos que* p *ramifica em* $\mathbb{K}$.

(iii) Se $m = 1, e_1 = 1, f(\mathcal{Q}_1|P) = 2$, *então* $p\mathcal{O}_{\mathbb{K}} = \mathcal{Q}_1$. *Dizemos que* p *é inerte em* $\mathbb{K}$.

Se $p \in \mathbb{Z}$ é um número primo e $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, um outro modo de verificar como se dá a fatoração de ideais primos em $\mathbb{K}$, que relaciona o símbolo de Kronecker e o discriminante é:

$$(p) \text{ se fatora em } \mathbb{K} \text{ se, e somente se, } \left(\frac{\mathcal{D}_{\mathbb{K}}}{p}\right) = 1,$$

$$(p) \text{ ramifica em } \mathbb{K} \text{ se, e somente se, } \left(\frac{\mathcal{D}_{\mathbb{K}}}{p}\right) = 0,$$

$$(p) \text{ é inerte em } \mathbb{K} \text{ se, e somente se, } \left(\frac{\mathcal{D}_{\mathbb{K}}}{p}\right) = -1.$$

4.4 Número de Classe

Apresentamos nesta seção o conceito de número de classe e alguns resultados envolvendo este conceito que serão usados no Capítulo 6.

Definição 4.17. *Seja $\mathbb{K}$ um corpo de números e $I(\mathbb{K})$ o grupo dos ideais fracionários não-nulos. Seja $P(\mathbb{K})$ o subgrupo dos ideais principais de $I(\mathbb{K})$. Então o grupo $\frac{I(\mathbb{K})}{P(\mathbb{K})}$ é chamado de* ***grupo de classe*** *de $\mathbb{K}$ e é denotado por $H(\mathbb{K})$.*

Um resultado importante, que é consequência de alguns teoremas de Hermann Minkowski (1864-1909) na geometria dos números, é que $H(\mathbb{K})$ é sempre um grupo finito, conforme [1].

Definição 4.18. *Seja $\mathbb{K}$ um corpo de números. A ordem de $H(\mathbb{K})$ é chamada de* ***número de classe*** *de $\mathbb{K}$ e é denotada por $h(\mathbb{K})$.*

Teorema 4.6. *Seja $\mathbb{K}$ um corpo de números. Então, $h(\mathbb{K}) = 1$ se, e somente se, $\mathcal{O}_{\mathbb{K}}$ é um domínio de ideais principais.*

Demonstração. Se $h(\mathbb{K}) = 1$ então

$$[I(\mathbb{K}) : P(\mathbb{K})] = \# \left(\frac{I(\mathbb{K})}{P(\mathbb{K})} \right) = \#H(\mathbb{K}) = h(\mathbb{K}) = 1$$

e portanto $P(\mathbb{K}) = I(\mathbb{K})$.

Por outro lado, se $\mathcal{O}_{\mathbb{K}}$ é um domínio de ideais principais, então todo ideal de $\mathcal{O}_{\mathbb{K}}$ é principal e portanto $I(\mathbb{K}) = P(\mathbb{K})$. Daí,

$$h(\mathbb{K}) = \#H(\mathbb{K}) = \# \left(\frac{I(\mathbb{K})}{P(\mathbb{K})} \right) = [I(\mathbb{K}) : P(\mathbb{K})] = 1.$$

□

No que segue apresentamos um algoritmo para encontrar o grupo de classe $H(\mathbb{K})$ de um corpo de números $\mathbb{K}$ (ver [1]) a saber:

Entrada: Corpo de números $\mathbb{K} = \mathbb{Q}(\theta)$.

Passo 1: Determine $n = [\mathbb{K} : \mathbb{Q}]$.

Passo 2: Determine r o número de conjugados reais de θ. Então faça $s = \frac{1}{2}(n - r)$.

Passo 3: Determine $\mathcal{D}_{\mathbb{K}}$, o discriminante de $\mathbb{K}$.

Passo 4: Calcule o limitante de Minkowski $M_{\mathbb{K}} = (2/\pi)^s \sqrt{|\mathcal{D}_{\mathbb{K}}|}$.

Passo 5: Determine todos os primos $p \leq M_{\mathbb{K}}$.

Passo 6: Determine a fatoração em ideais primos de cada ideal principal $\langle p \rangle$ em $\mathcal{O}_{\mathbb{K}}$ com p como no Passo 5.

Passo 7: Determine todos os produtos desses ideais primos que têm norma $\leq M_{\mathbb{K}}$.

Passo 8: Determine os geradores de $H(\mathbb{K})$ a partir das classes destes produtos.

Saída: $H(\mathbb{K})$.

Exemplo 4.8. Vamos mostrar que $\mathbb{K} = \mathbb{Q}(\sqrt{-19})$ tem número de classe $h(\mathbb{K}) = 1$. Neste caso tem-se que,

$$n = 2,\ r = 0,\ s = 1\ e\ \mathcal{D}_{\mathbb{K}} = -19.$$

O limitante de Minkowski é

$$M_{\mathbb{K}} = \left(\frac{2}{\pi}\right)^{s} \sqrt{|\mathcal{D}_{\mathbb{K}}|} = \frac{2}{\pi}\sqrt{19} < \frac{2}{3}.5 < 4,$$

de modo que os primos $p \leq M_{\mathbb{K}}$ são $p = 2$ e $p = 3$. Como

$$\left(\frac{-19}{2}\right) = \left(\frac{-19}{3}\right) = -1,$$

os ideais principais $\langle 2\rangle$ e $\langle 3\rangle$ são inertes em $\mathcal{O}_{\mathbb{K}}$, portanto são ambos ideais primos de $\mathcal{O}_{\mathbb{K}}$. Assim todo ideal primo de $\mathcal{O}_{\mathbb{K}}$ é principal. Portanto, pelo Teorema 4.6 $h(\mathbb{K}) = h(\mathbb{Q}(\sqrt{-19})) = 1$.

Tabela 4.1: Número de classes de corpos quadráticos imaginários

$\mathbb{K} = \mathbb{Q}(\sqrt{k}),\ -195 \leq k < 0, k$ *livre de quadrados*

k	$h(\mathbb{K})$	k	$h(\mathbb{K})$	k	$h(\mathbb{K})$	k	$h(\mathbb{K})$	k	$h(\mathbb{K})$
-1	1	-38	6	-78	4	-115	2	-158	8
-2	1	-39	4	-79	5	-118	6	-159	10
-3	1	-41	8	-82	4	-119	10	-161	16
-5	2	-42	4	-83	3	-122	10	-163	1
-6	2	-43	1	-85	4	-123	2	-165	8
-7	1	-46	4	-86	10	-127	5	-166	10
-10	2	-47	5	-87	6	-129	12	-167	11
-11	1	-51	2	-89	12	-130	4	-170	12
-13	2	-53	6	-91	2	-131	5	-173	14
-14	4	-55	4	-93	4	-133	4	-174	12
-15	2	-57	4	-94	8	-134	14	-177	4
-17	4	-58	2	-95	8	-137	8	-178	8
-19	1	-59	3	-97	4	-138	8	-179	5
-21	4	-61	6	-101	14	-139	3	-181	10
-22	2	-62	8	-102	4	-141	8	-182	12
-23	3	-65	8	-103	5	-142	4	-183	8
-26	6	-66	8	-105	8	-143	10	-185	16
-29	6	-67	1	-106	6	-145	8	-186	12
-30	4	-69	8	-107	3	-146	16	-187	2
-31	3	-70	4	-109	6	-149	14	-190	4
-33	4	-71	7	-110	12	-151	7	-191	13
-34	4	-73	4	-111	8	-154	8	-193	4
-35	2	-74	10	-113	8	-155	4	-194	20
-37	2	-77	8	-114	8	-157	6	-195	4

Tabela 4.2: Números de classe de corpos quadráticos reais

$\mathbb{K} = \mathbb{Q}(\sqrt{k}),\ 0 < k \leq 197, k$ *livre de quadrados*

k	$h(\mathbb{K})$	k	$h(\mathbb{K})$	k	$h(\mathbb{K})$	k	$h(\mathbb{K})$	k	$h(\mathbb{K})$
2	1	39	2	79	3	118	1	159	2
3	1	41	1	82	4	119	2	161	1
5	1	42	2	83	1	122	2	163	1
6	1	43	1	85	2	123	2	165	2
7	1	46	1	86	1	127	1	166	1
10	2	47	1	87	2	129	1	167	1
11	1	51	2	89	1	130	4	170	4
13	1	53	1	91	2	131	1	173	1
14	1	55	2	93	1	133	1	174	2
15	2	57	1	94	1	134	1	177	1
17	1	58	2	95	2	137	1	178	2
19	1	59	1	97	1	138	2	179	1
21	1	61	1	101	1	139	1	181	1
22	1	62	1	102	2	141	1	182	2
23	1	65	2	103	1	142	3	183	2
26	2	66	2	105	2	143	2	185	2
29	1	67	1	106	2	145	4	186	2
30	2	69	1	107	1	146	2	187	2
31	1	70	2	109	1	149	1	190	2
33	1	71	1	110	2	151	1	191	1
34	2	73	1	111	2	154	2	193	1
35	2	74	2	113	1	155	2	194	2
37	1	77	1	114	2	157	1	195	4
38	1	78	2	115	2	158	1	197	1

Tabela 4.3: Número de classes de corpos ciclotômicos $\mathbb{Q}(\zeta_m)$

$3 \leq m \leq 45,\ m \not\equiv 2(mod\ 4)$

m	$h(\mathbb{Q}(\zeta_m))$	m	$h(\mathbb{Q}(\zeta_m))$	m	$h(\mathbb{Q}(\zeta_m))$
3	1	17	1	32	1
4	1	19	1	33	1
5	1	20	1	35	1
7	1	21	1	36	1
8	1	23	3	37	37
9	1	24	1	39	2
11	1	25	1	40	1
12	1	27	1	41	121
13	1	28	1	43	211
15	1	29	8	44	1
16	1	31	9	45	1

$\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ para n ímpar.

5 Aplicação 1: Reticulados

Neste capítulo apresentamos um método para a geração de reticulados no $\mathbb{R}^n$. A vantagem de obter reticulados por este método é que podemos identificar os pontos do reticulado no $\mathbb{R}^n$ como os elementos de um corpo de números. As principais referências utilizadas foram [3], [8], [11], [13] e [15].

5.1 Reticulados

Intuitivamente, entende-se por reticulado um subconjunto discreto do $\mathbb{R}^n$ que tem a estrutura de um $\mathbb{Z}$-módulo (que é equivalente a ser um grupo abeliano aditivo) de posto finito n. Nesta seção apresentamos a definição de reticulados e outras definições importantes como a região fundamental, matriz de Gram e volume da região fundamental.

Definição 5.1. *Sejam $\{v_1, v_2, ..., v_m\}$ vetores linearmente independentes do $\mathbb{R}^n$. O conjunto de pontos*

$$\Lambda = \left\{ \mathbf{x} = \sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z} \right\},$$

*é chamado **reticulado** de dimensão m e $\{v_1, v_2, ..., v_m\}$ é chamado de **base** do reticulado.*

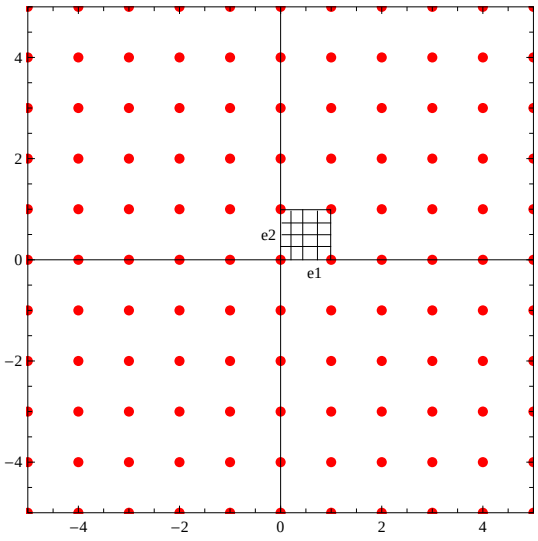
Observe que na definição 5.1, necessariamente $m \leq n$.

Definição 5.2. *O paralelepípedo formado pelos pontos*

$$\theta_1 v_1 + \cdots + \theta_m v_m, \ 0 \leq \theta_i < 1,$$

é chamado um **paralelepípedo fundamental** *ou* **região fundamental** *do reticulado.*

Exemplo 5.1. $\Lambda = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$ com região fundamental descrita na figura a seguir.



Definição 5.3. *Seja* $\{v_1, \ldots, v_m\}$ *uma base do reticulado* Λ. *Se* $v_i = (v_{i1}, \ldots, v_{in})$, *para* $i = 1, \cdots, m$, *a matriz*

$$M = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ & & \ddots & \\ v_{m1} & v_{m2} & \ldots & v_{mn} \end{pmatrix}$$

é chamada uma ***matriz geradora*** *para o reticulado. A matriz* $G = MM^t$ *é chamada uma* ***matriz de Gram*** *para o reticulado, onde* t *denota a transposição e o* ***volume*** *de* Λ *é dado por* $vol(\Lambda) = |det\ (M)|$.

Observação 5.1. De acordo com a Definição 5.3, os pontos do reticulado são formados por

$$\Lambda = \{\mathbf{x} = \lambda M | \lambda \in \mathbb{Z}^m\}.$$

Definição 5.4. *O* ***determinante do reticulado*** Λ *é definido como sendo o determinante da matriz* G

$$det(\Lambda) = det(G).$$

Definição 5.5. *Um* **empacotamento esférico**, *ou simplesmente um empacotamento no* $\mathbb{R}^n$, *é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

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

$$\Delta(\Lambda) = \frac{\mathcal{V}ol(\mathcal{B}(1))\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por

$$\delta(\Lambda) = \frac{\rho^n}{\mathcal{V}ol(\Lambda)}.$$

Um dos problemas de empacotamento esférico de um reticulado no $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade. Os reticulados nas dimensões 1 a 8 e 24 são os reticulados com maior densidade de empacotamento conhecidos.

5.2 Reticulados Algébricos

Definição 5.6. *Seja $\sigma_1, \cdots, \sigma_n$ os n $\mathbb{Q}$-monomorfismos de um corpo de números $\mathbb{K}$ de grau n, e vamos ordenar os σ_is de modo que, para todo $x \in \mathbb{K}$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, e $\sigma_{j+r_2}(x)$ é o conjugado complexo de $\sigma_j(x)$ para $r_1 + 1 \leq j \leq r_1 + r_2$. Note que $r_1 + 2r_2 = n$. Chamamos de* **monomorfismo canônico** *$\sigma : \mathbb{K} \longrightarrow \mathbb{R}^{r_1+2r_2}$ definido por*

$$\sigma(x) = (\sigma_1(x), \cdots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \cdots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)),$$

onde $\Re$ e $\Im$ denotam as partes real e imaginária, respectivamente.

Exemplo 5.2. Sejam o corpo quadrático $\mathbb{K} = \mathbb{Q}(i)$, onde $i = \sqrt{-1}$, e $\{\sigma_1, \sigma_2\}$ o grupo dos $\mathbb{Q}$-monomorfismos de $\mathbb{K}$ em $\mathbb{C}$, onde σ_1 é a aplicação identidade e $\sigma_2(a+bi) = a-bi$, com $a, b \in \mathbb{Q}$. Neste caso, $r_1 = 0$ e $r_2 = 1$. Para $x = a + bi \in \mathbb{K}$, com $a, b \in \mathbb{Q}$, temos $\sigma(x) = (\Re\sigma_1(x), \Im\sigma_1(x)) = (a, b)$.

Uma das aplicações deste monomorfismo é a geração de reticulados no $\mathbb{R}^n$, onde os principais parâmetros podem ser obtidos via teoria dos números algébricos, através de propriedades herdadas de $\mathbb{K}$. Isto pode ser visto de maneira formal no resultado que segue.

Teorema 5.1. *Se $\{w_1, \cdots, w_n\}$ é uma base integral de $\mathbb{K}$ e $\sigma : \mathbb{K} \to \mathbb{C}$ o monomorfismo canônico, então os n vetores $\mathbf{v_i} = \sigma(w_i) \in \mathbb{R}^n$, $i = 1, \cdots, n$ são linearmente independentes e definem um reticulado em $\mathbb{R}^n$, denominado* **reticulado algébrico**.

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

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

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

Proposição 5.1. *[11] Se $\mathbb{K}$ é um corpo de números de grau n, $\mathcal{D}_\mathbb{K}$ o discriminante de $\mathbb{K}$, $\mathcal{O}_\mathbb{K}$ o anel dos inteiros algébricos de $\mathbb{K}$, I um ideal não nulo de $\mathcal{O}_\mathbb{K}$ e r_2 a metade no número de monomorfismos imaginários, então, $\sigma_\mathbb{K}(\mathcal{O}_\mathbb{K})$ e $\sigma_\mathbb{K}(I)$ são reticulados, com respectivos volumes,*

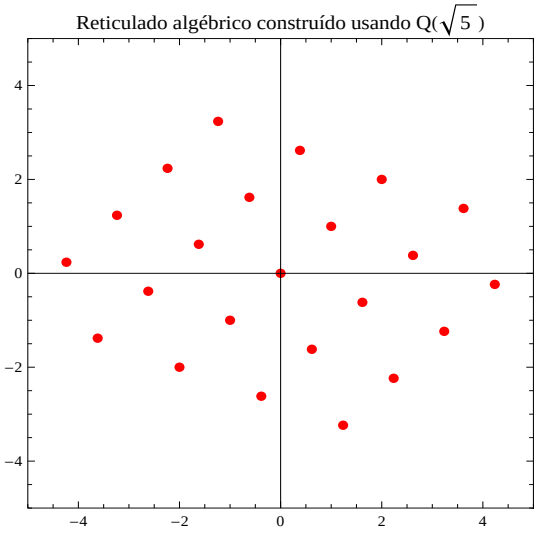
$$Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-r_2}|\mathcal{D}_{\mathbb{K}}|^{\frac{1}{2}},$$
$$Vol(\sigma_{\mathbb{K}}(I)) = Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))N(I).$$

Exemplo 5.3. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. A base integral de $\mathbb{K}$ é $\{1, \frac{1+\sqrt{5}}{2}\}$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Pelo Teorema (5.1), $\Lambda = \sigma(\mathcal{O}_{\mathbb{K}})$ é um reticulado no $\mathbb{R}^2$. Os dois monomorfismos são $\sigma_1(\sqrt{5}) = \sqrt{5}$, $\sigma_2(\sqrt{5}) = -\sqrt{5}$. Neste caso, $r_1 = 2$ e $r_2 = 0$, assim a matriz geradora do reticulado é

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_2(1) \\ \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}.$$

e volume dado por

$$Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-0}\left|\left[det\begin{pmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{5}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix}\right]^2\right|^{\frac{1}{2}} = \left|det\begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}\right| = \sqrt{5}.$$

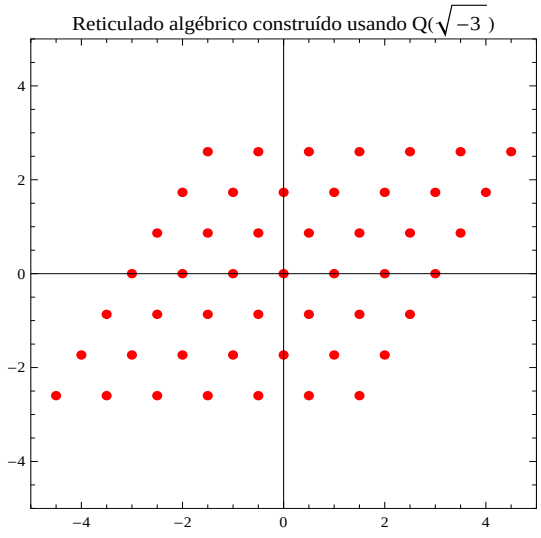


Exemplo 5.4. Seja $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. A base integral de $\mathbb{K}$ é $\{1, \frac{1+\sqrt{-3}}{2}\}$ e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$. Pelo Teorema (5.1), $\Lambda = \sigma(\mathcal{O}_{\mathbb{K}})$ é um reticulado no $\mathbb{R}^2$. Os dois monomorfismos são $\sigma_1(\sqrt{-3}) = \sqrt{-3}$, $\sigma_2(\sqrt{-3}) = -\sqrt{-3}$. Neste caso, $r_1 = 0$ e $r_2 = 1$, assim, a matriz geradora do reticulado é

$$M = \begin{pmatrix} \Re\sigma_1(1) & \Im\sigma_1(1) \\ \Re\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) & \Im\sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix},$$

e volume dado por

$$\begin{aligned} Vol(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) &= 2^{-1}\left|\left[det\begin{pmatrix} \sigma_1(1) & \sigma_1\left(\frac{1+\sqrt{-3}}{2}\right) \\ \sigma_2(1) & \sigma_2\left(\frac{1+\sqrt{-3}}{2}\right) \end{pmatrix}\right]^2\right|^{\frac{1}{2}} = \frac{1}{2}\left|det\begin{pmatrix} 1 & \frac{1+\sqrt{-3}}{2} \\ 1 & \frac{1-\sqrt{-3}}{2} \end{pmatrix}\right| \\ &= \frac{1}{2}|-i\sqrt{3}| = \frac{1}{2}\sqrt{3}. \end{aligned}$$



É possível verificar que com essa estrutura algébrica obtêm-se o reticulado hexagonal A_2. Para maiores detalhes consultar [13].

6 Aplicação 2: Solução da Equação Diofantina $y^2 = x^3 + k$

Uma equação com coeficientes inteiros e que deve ser resolvida em números inteiros é chamada de equação Diofantina, em honra a Diofanto (200-284 d.C). Não se sabe muito sobre Diofanto, mas sabe-se que ele propôs em seus principais trabalhos aritméticos muitos problemas a serem resolvidos em números racionais ou inteiros, segundo [1].

Por exemplo, se considerarmos a equação $3x + 2y = 7$, observe que $3 - 2 = 1$ e multiplicando ambos os lados da equação por 7 obtemos que $3(7) + 2(-7) = 7$. Assim $(7, -7)$ é solução da equação. Portanto a equação $3x + 2y = 7$ é uma equação Diofantina, pois possui coeficientes e solução inteiras.

Neste capítulo, vamos aplicar a teoria dos números algébricos para resolver a equação Diofantina:

$$y^2 = x^3 + k$$

onde k é um inteiro qualquer.

Esta equação é muitas vezes chamada de equação de Bachet, em homenagem ao matemático francês Claude Gaspard Bachet de M'eziriac (1581-1683), que mostrou como encontrar soluções de $y^2 = x^3 - 2$ para $x, y \in \mathbb{Q}$. Em 1917, Axel Thue (1863-1922), mostrou que para um dado inteiro k diferente de zero, a equação de Bachet tem no máximo um número finito de soluções para $x, y \in \mathbb{Z}$. Portanto, o problema de encontrar todas as soluções em inteiros da equação de Bachet para um dado inteiro não nulo k é reduzida a uma busca finita.

6.1 Solução de $y^2 = x^3 + k$ via Teoria dos Números Algébricos

Nesta seção, usamos a aritmética dos corpos quadráticos para determinar todas as soluções em inteiros (se houver) da equação de Bachet para certos valores de k. Em particular quando $k = -2$ mostramos que $(x, y) = (3, \pm 5)$ são as únicas soluções em números inteiros de $y^2 = x^3 - 2$, este é o primeiro resultado estabelecido por Fermat.

Os principais resultados que usaremos são os dois teoremas que seguem.

Teorema 6.1. *[1] Seja D um domínio de Dedekind. Sejam A, B e C ideais diferentes de zero de D tal que A e B são coprimos ($A + B = \langle 1 \rangle$) e*

$$AB = C^n,$$

onde n é um inteiro positivo. Nestas condições existem ideais A_1 e B_1 de D tais que

$$A = A_1^n, B = B_1^n \text{ e } C = A_1 B_1.$$

Demonstração. Como D é um domínio de Dedekind, cada ideal diferente de zero de D pode ser expresso unicamente como um produto de ideais primos (Teorema 4.3). Assim

$$C = P_1^{a_1} \cdots P_r^{a_r},$$

onde $P_1, ..., P_r$ são ideais primos distintos e $a_1, ..., a_r$ são inteiros positivos. Daí

$$AB = P_1^{na_1} \cdots P_r^{na_r}.$$

Como A e B são ideais primos entre si, cada potência primária $P_i^{na_i}$ $(i = 1, ..., r)$ divide A ou B, mas não ambos. Daí reorganizando as potências se necessário temos

$$A = P_1^{na_1} \cdots P_s^{na_s} \text{ e } B = P_{s+1}^{na_{s+1}} \cdots P_r^{na_r},$$

para algum inteiro s com $0 \leq s \leq r$. Sejam $A_1 = P_1^{a_1} \cdots P_s^{a_s}$ e $B_1 = P_{s+1}^{a_{s+1}} \cdots P_r^{a_r}$, então $A = A_1^n$, $B = B_1^n$, e $C = A_1 B_1$ como queríamos. □

Como o anel de inteiros de um corpo de números é um domínio de Dedekind, o Teorema 6.1 aplica-se neste caso.

Teorema 6.2. *[1] Se $\mathbb{K}$ é um corpo de números, h o número de classes de $\mathbb{K}$ e A um ideal de $\mathcal{O}_{\mathbb{K}}$ tal que A^k é um ideal principal para algum inteiro positivo k coprimo com h, então A é um ideal principal.*

Demonstração. Denotemos por $[A]$ a classe lateral A em $H(\mathbb{K})$. Como a ordem de $H(\mathbb{K})$ é h, temos $[A]^h = I$ assim A^h é um ideal principal. Como $mdc(h, k) = 1$ existem inteiros r e s tal que $rh + sk = 1$. Então, como A^k é um ideal principal, temos

$$A = A^{rh+sk} = (A^h)^r (A^k)^s$$

e portanto A é um ideal principal. □

Vamos agora esboçar as ideias envolvidas nas utilizações dos Teoremas (6.1) e (6.2) para obter classes de números inteiros k para quais podemos encontrar soluções (se houver) da equação Diofantina $y^2 = x^3 + k$.

Começamos supondo que a equação $y^2 = x^3 + k$ tem solução em inteiros x e y, de modo que

$$x^3 = (y + \sqrt{k})(y - \sqrt{k}).$$

Notemos que $y + \sqrt{k}$ e $y - \sqrt{k}$ são inteiros algébricos do corpo quadrático $\mathbb{K} = \mathbb{Q}(\sqrt{k})$. Vamos assumir que k é livre de quadrados e que $k \equiv 2(mod\ 4)$ ou $k \equiv 3(mod\ 4)$ para evitar que o número 2 esteja nos denominadores dos inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{k})$, pelo Teorema 3.1 $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{k}]$.

Passando para ideais em $\mathcal{O}_{\mathbb{K}}$, obtemos

$$\langle x \rangle^3 = \langle y + \sqrt{k} \rangle \langle y - \sqrt{k} \rangle.$$

Se os valores de k são escolhidos de modo que os ideias principais $\langle y + \sqrt{k} \rangle$ e $\langle y - \sqrt{k} \rangle$ são primos entre si, então podemos deduzir do Teorema 6.1 que

$$\langle y + \sqrt{k} \rangle = A^3$$

para algum ideal A de $\mathcal{O}_{\mathbb{K}}$. Além disso, se o número da classe de $\mathbb{K}$ não é divisível por 3, sabemos pelo Teorema 6.2 que A é um ideal principal, digamos

$$A = \langle a + b\sqrt{k} \rangle$$

para algum inteiro a e b. Logo

$$\langle y + \sqrt{k} \rangle = \langle a + b\sqrt{k} \rangle^3 = \langle (a + b\sqrt{k})^3 \rangle$$

e pelo Teorema 4.1

$$y + \sqrt{k} = \epsilon(a + b\sqrt{k})^3,$$

onde ϵ é uma unidade de $\mathcal{O}_{\mathbb{K}}$. Dois casos surgem dependendo se k é negativo ou positivo.

Se k é negativo, então há apenas um número finito de possibilidades para ϵ. De fato, se $k \neq -1$ então $\epsilon = \pm 1$ e se $k = -1$ então $\epsilon = \pm 1, \pm i$ (Teorema 3.2). Uma vez que os cubos podem ser absorvidos em $(a + b\sqrt{k})^3$ e $-1 = (-1)^3$, $i = (-i)^3$ e $-i = i^3$, a equação torna-se

$$y + \sqrt{k} = (\tilde{a} + \tilde{b}\sqrt{k})^3.$$

Igualando os coeficientes de $\sqrt{k}$, obtemos

$$1 = 3\tilde{a}^2\tilde{b} + k\tilde{b}^3 = \tilde{b}(3\tilde{a}^2 + k\tilde{b}^2),$$

de modo que $\tilde{b} = \pm 1$. Agora é uma questão de determinar as possibilidades de a, e consequentemente as soluções x, y em números inteiros para $y^2 = x^3 + k$ (veja Teorema 6.3).

Se k é positivo, então existem infinitas possibilidades para ϵ. De fato, $\epsilon = \pm\eta^\ell$, onde $\eta = T + U\sqrt{k}(> 1)$ é a unidade fundamental de $\mathcal{O}_\mathbb{K}$ e $\ell \in \mathbb{Z}$ (Teorema 3.3). Absorvendo os cubos $-1 = (-1)^3$ e $\eta^{3m} = (\eta^m)^3$ em $(\tilde{a} + \tilde{b}\sqrt{k})^3$ vemos que temos somente que examinar as três equações

$$y + \sqrt{k} = (\tilde{a} + \tilde{b}\sqrt{k})^3,$$
$$y + \sqrt{k} = \eta(\tilde{a} + \tilde{b}\sqrt{k})^3$$

e

$$y + \sqrt{k} = \eta^2(\tilde{a} + \tilde{b}\sqrt{k})^3.$$

A primeira destas equações pode ser tratada como no caso $k < 0$. Para as outras duas equações é conveniente impor condições de congruência em k, T e U para garantir que ela não têm quaisquer soluções. Isto é ilustrado no Teorema 6.4. Devemos notar que os cubos absorvidos devem ser levados em conta quando se procura todas as soluções de $y^2 = x^3 + k$.

Teorema 6.3. *Seja k um inteiro tal que $k < -1$ e livre de quadrados, $k \equiv 2 (mod\ 4)$ ou $k \equiv 3 (mod\ 4)$ e $h(\mathbb{Q}(\sqrt{k})) \not\equiv 0 (mod\ 3)$.*

(a) Se existe um número inteiro a tal que

$$k = 1 - 3a^2,$$

então as únicas soluções em inteiros de $y^2 = x^3 + k$ são

$$x = 4a^2 - 1,\ y = \pm(3a - 8a^3).$$

(b) Se existe um número inteiro a tal que

$$k = -1 - 3a^2,$$

então as únicas soluções em inteiros de $y^2 = x^3 + k$ são

$$x = 4a^2 + 1,\ y = \pm(3a + 8a^3).$$

(c) Se $k \neq \pm 1 - 3a^2$ para qualquer inteiro a, então $y^2 = x^3 + k$ não tem soluções em inteiros x e y.

Demonstração. Suponha que $y^2 = x^3 + k$ tem uma solução x e y em inteiros e vamos mostrar que ou o caso (a) ou o caso (b) vale. (Observamos que, no caso (a) $k \equiv 1(mod\ 3)$ e no caso (b) $k \equiv 2(mod\ 3)$, de modo que os casos (a) e (b) são exclusivos.)

Primeiramente, vamos mostrar que $x \equiv 1(mod\ 2)$. Como $y^2 \equiv 0(mod\ 4)$ ou $y^2 \equiv 1(mod\ 4)$ e $k \equiv 2(mod\ 4)$ ou $k \equiv 3(mod\ 4)$ por hipótese, vemos que $x^3 = y^2 - k \equiv 1(mod\ 4)$ ou $x^3 = y^2 - k \equiv 2(mod\ 4)$ ou $x^3 = y^2 - k \equiv 3(mod\ 4)$. Mas $x^3 \not\equiv 2(mod\ 4)$ pois $y^2 \not\equiv 1(mod\ 4)$ assim $x^3 \equiv 1(mod\ 4)$ ou $x^3 \equiv 3(mod\ 4)$, consequentemente $x \equiv 1(mod\ 2)$.

Em seguida, vamos provar que $mdc(x, k) = 1$. Suponha que $mdc(x, k) \neq 1$, então existe um primo p tal que $p \mid x$ e $p \mid k$. Como k é livre de quadrados temos $p^2 \nmid k$. Assim, $p \nmid x^3 + k$ e então $p \nmid y^2$, uma contradição.

De $x \equiv 1(mod\ 2)$ e $mdc(x, k) = 1$ deduzimos que $mdc(x, 2k) = 1$ e portanto existem $l, m \in \mathbb{Z}$ tais que

$$lx + m(2k) = 1. \tag{6.1}$$

Agora, seja $\mathbb{K} = \mathbb{Q}(\sqrt{k})$ de modo que $\mathbb{K}$ seja um corpo quadrático imaginário. Como $k \equiv 2(mod\ 4)$ ou $k \equiv 3(mod\ 4)$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ é $\mathbb{Z}[\sqrt{d}]$. Mostraremos que os ideais principais $\langle y + \sqrt{k}\rangle$ e $\langle y - \sqrt{k}\rangle$ de $\mathcal{O}_{\mathbb{K}}$ são primos entre si. Suponha que não são primos entre si, então existe um ideal primo P tal que

$$P \mid \langle y + \sqrt{k}\rangle \ e \ P \mid \langle y - \sqrt{k}\rangle.$$

Assim,

$$y + \sqrt{k} \in P \ e \ y - \sqrt{k} \in P.$$

Então

$$2\sqrt{k} = (y + \sqrt{k}) - (y - \sqrt{k}) \in P$$

e assim

$$2k = \sqrt{k}(2\sqrt{k}) \in P. \tag{6.2}$$

Agora,

$$\langle y + \sqrt{k}\rangle\langle y - \sqrt{k}\rangle = \langle y^2 - k\rangle = \langle x^3\rangle = \langle x\rangle^3$$

de modo que

$$P \mid \langle x\rangle^3.$$

Como P é um ideal primo, deduzimos que

$$P \mid \langle x \rangle.$$

Portanto

$$x \in P. \tag{6.3}$$

De (6.1) e (6.3), vemos que $1 \in P$, contradizendo que P é um ideal primo.

Mostramos portanto que $\langle y + \sqrt{k} \rangle$ e $\langle y - \sqrt{k} \rangle$ são ideais primos entre si de $\mathcal{O}_{\mathbb{K}}$ com $\langle y + \sqrt{k} \rangle \langle y - \sqrt{k} \rangle = \langle x \rangle^3$. Como $\mathbb{K}$ é um corpo de números, $\mathcal{O}_{\mathbb{K}}$ é um domínio de Dedekind e portanto pelo Teorema 6.1, existe um ideal A de $\mathcal{O}_{\mathbb{K}}$ tal que

$$\langle y + \sqrt{k} \rangle = A^3.$$

Portanto A^3 é um ideal principal e, como $h(\mathbb{Q}(\sqrt{k})) \not\equiv 0 (mod\ 3)$ segue que 3 é coprimo com $h(\mathbb{Q}(\sqrt{k}))$ e pelo Teorema 6.2, A é um ideal principal, digamos

$$A = \langle a + b\sqrt{k} \rangle,$$

onde $a, b \in \mathbb{Z}$. Assim

$$\langle y + \sqrt{k} \rangle = \langle a + b\sqrt{k} \rangle^3 = \langle (a + b\sqrt{k})^3 \rangle.$$

Pelo Teorema 4.1 existe uma unidade $\epsilon \in \mathcal{O}_{\mathbb{K}}$ tal que

$$y + \sqrt{k} = \epsilon(a + b\sqrt{k})^3. \tag{6.4}$$

Como $k < -1$, $k \equiv 2 (mod\ 4)$ ou $k \equiv 3 (mod\ 4)$ pelo Teorema 3.2 segue que $\epsilon = \pm 1$. Tomando o conjugado em (6.4), obtemos

$$y - \sqrt{k} = \epsilon(a - b\sqrt{k})^3. \tag{6.5}$$

Portanto

$$x^3 = y^2 - k = (y + \sqrt{k})(y - \sqrt{k}) = (a + b\sqrt{k})^3 (a - b\sqrt{k})^3 =$$
$$= ((a + b\sqrt{k})(a - b\sqrt{k}))^3 = (a^2 - kb^2)^3.$$

Assim

$$x = a^2 - kb^2. \tag{6.6}$$

Adicionando e subtraindo (6.4) e (6.5), obtemos

$$2y = \epsilon((a + b\sqrt{k})^3 + (a - b\sqrt{k})^3)$$

e

$$2\sqrt{k} = \epsilon((a + b\sqrt{k})^3 - (a - b\sqrt{k})^3),$$

de modo que

$$y = \epsilon(a^3 + 3kab^2) \; e \; 1 = \epsilon(3a^2b + kb^3).$$

De $1 = \epsilon b(3a^2 + kb^2)$ vemos que $\epsilon b = \pm 1$, assim $b = \pm\epsilon$. Se $b = \epsilon$ então

$$x = a^2 - k, y = \epsilon(a^3 + 3ka) \; e \; 1 = 3a^2 + k,$$

logo,

$$k = 1 - 3a^2$$

e

$$x = 4a^2 - 1 \; e \; y = \pm(3a - 8a^3).$$

Claramente,

$$x^3 + k = (4a^2 - 1)^3 + (1 - 3a^2) = 64a^6 - 48a^4 + 9a^2 = (8a^3 - 3a)^2 = y^2.$$

Se $b = -\epsilon$ então

$$x = a^2 - k, y = \epsilon(a^3 + 3ka) \; e \; 1 = -3a^2 - k,$$

logo,

$$k = -1 - 3a^2$$

e

$$x = 4a^2 + 1 \; e \; y = \pm(3a + 8a^3).$$

Claramente

$$x^3 + k = (4a^2 + 1)^3 - 1 - 3a^2 = 64a^6 + 48a^4 + 9a^2 = (8a^3 + 3a)^2 = y^2.$$

Isso completa a demonstração do teorema. □

Exemplo 6.1. O inteiro $k = -2 = 1 - 3.1^2$ satisfaz as condições do Teorema 6.3(a). Como $h(\mathbb{Q}(\sqrt{-2})) = 1$, segue que as únicas soluções em inteiros para a equação

$$y^2 = x^3 - 2$$

são $(x, y) = (3, \pm 5)$. Este resultado foi afirmado primeiro por Fermat.

Os valores de k no intervalo $-200 < k < -2$ que satisfazem as condições do Teorema 6.3(a) são

$$k = -74 = 1 - 3.5^2 \quad (h(\mathbb{Q}(\sqrt{-74})) = 10)$$

e

$$k = -146 = 1 - 3.7^2 \quad (h(\mathbb{Q}(\sqrt{-146})) = 16).$$

Assim, pelo Teorema 6.3(a), as únicas soluções em inteiros de $y^2 = x^3 - 74$ são $(x, y) = (99, \pm 985)$ e as únicas soluções em inteiros de $y^2 = x^3 - 146$ são $(x, y) = (195, \pm 2723)$.

Exemplo 6.2. O menor número inteiro k em valor absoluto que satisfaz as condições do Teorema 6.3(b) é

$$k = -13 = -1 - 3.2^2$$

pois $h(\mathbb{Q}(\sqrt{-13})) = 2$. Assim, pelo Teorema 6.3(b), as únicas soluções em inteiros x e y da equação

$$y^2 = x^3 - 13$$

são $(x, y) = (17, \pm 70)$. No intervalo $-200 < k < -1$ há apenas um outro valor de k que satisfaz as condições do Teorema 6.3(b), que é

$$k = -193 = -1 - 3.8^2 \quad (h(\mathbb{Q}(\sqrt{-193})) = 4).$$

As únicas soluções em inteiros da equação $y^2 = x^3 - 193$ são $(x, y) = (257, \pm 4120)$.

Exemplo 6.3. O número inteiro $k = -5$ satisfaz as condições do Teorema 6.3(c) pois $h(\mathbb{Q}(\sqrt{-5})) = 2$. Assim a equação

$$y^2 = x^3 - 5$$

não tem soluções em inteiros.

Da mesma forma, encontramos que $y^2 = x^3 + k$ não tem solução em números inteiros x e y para

$$k = -6, -10, -14, -17, -21, -22.$$

No próximo teorema, apresentamos um resultado semelhante ao do Teorema 6.3(c) no caso em que k é positivo.

Teorema 6.4. *Seja k um número inteiro tal que $k > 0$ e livre de quadrados, $k \equiv 2(mod\ 4)$ ou $k \equiv 3(mod\ 4), h(\mathbb{Q}(\sqrt{k})) \not\equiv 0(mod\ 3)$ e $T + U\sqrt{k}$ a unidade fundamental de $\mathbb{K} = \mathbb{Q}(\sqrt{k})$ de norma 1. Nestas condições, se*

$$k \equiv 4(mod\ 9)\ e\ U \equiv 0(mod\ 9)$$

ou

$$k \equiv 7(mod\ 9)\ e\ U \equiv \pm 3(mod\ 9)$$

ou

$$k \equiv 4(mod\ 7)\ e\ U \equiv 0(mod\ 7)$$

então a equação $y^2 = x^3 + k$ não tem solução para $x, y \in \mathbb{Z}$.

Demonstração. Exatamente como na demonstração do Teorema 6.3, obtemos

$$y + \sqrt{k} = \epsilon(a + b\sqrt{k})^3,$$

onde ϵ é uma unidade de $\mathcal{O}_{\mathbb{K}}$. Seja η a unidade fundamental de $\mathcal{O}_{\mathbb{K}}$ de modo que

$$\epsilon = \pm\eta^{\ell}$$

para algum $l \in \mathbb{Z}$. Como os cubos $-1 = (-1)^3$ e $\eta^{3m} = (\eta^m)^3$ podem ser absorvidos no cubo $(a + b\sqrt{k})^3$, temos $y + \sqrt{k} = \epsilon(a + b\sqrt{k})^3$, onde $\epsilon = 1, \eta$ ou η^2. Além disso, como $\eta = \eta^3/\eta^2$ e $\eta^2 = \eta^3/\eta$, temos

$$y + \sqrt{k} = \epsilon(a + b\sqrt{k})^3,\ onde\ \epsilon \in \left\{1, \eta, \frac{1}{\eta}\right\}\ ou\ \left\{1, \frac{1}{\eta^2}, \eta^2\right\}.$$

Escolhemos $\epsilon \in \{1, \eta, 1/\eta\}$ se η tem norma 1 e $\epsilon \in \{1, 1/\eta^2, \eta^2\}$ se η tem norma -1. Assim em ambos os casos

$$\epsilon \in \{1, T + U\sqrt{k}, T - U\sqrt{k}\}.$$

onde $T + U\sqrt{k}$ é a unidade fundamental, maior que 1, de $\mathcal{O}_{\mathbb{K}}$ de norma 1. Se $\epsilon = 1$, igualando os coeficientes de $\sqrt{k}$ obtemos $1 = 3a^2b + kb^3$, assim $b \mid 1$ e então $b = \pm 1$. Portanto, $\pm 1 = b = 3a^2b^2 + kb^4 = 3a^2 + k \geq k > 1$, uma contradição. Assim, $\epsilon = T \pm U\sqrt{k}$. Então

$$y + \sqrt{k} = (T \pm U\sqrt{k})(a + b\sqrt{k})^3 =$$
$$= (T \pm U\sqrt{k})((a^3 + 3kab^2) + (3a^2b + kb^3)\sqrt{k}) =$$
$$= (T(a^3 + 3kab^2) \pm Uk(3a^2b + kb^3)) + (T(3a^2b + kb^3) \pm U(a^3 + 3kab^2))\sqrt{k}$$

de modo que,

$$1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2). \tag{6.7}$$

Caso (i): $k \equiv 4(mod\ 9)$ e $U \equiv 0(mod\ 9)$. Como $U \equiv 0(mod\ 9)$, para $T^2 - kU^2 = 1$ obtemos $T \equiv \pm 1(mod\ 81)$, digamos

$$T \equiv \epsilon(mod\ 81), \epsilon = \pm 1.$$

Então de (6.7) módulo 9, deduzimos que

$$1 \equiv \epsilon(3a^2b + 4b^3)(mod\ 9). \tag{6.8}$$

Claramente, essa congruência implica que $b \not\equiv 0(mod\ 3)$. Assim $b \equiv \pm 1(mod\ 3)$, digamos

$$b \equiv \lambda(mod\ 3), \lambda = \pm 1.$$

Logo,

$$b^3 \equiv \lambda(mod\ 9).$$

Então de (6.8) deduzimos que

$$1 \equiv \epsilon\lambda(3a^2 + 4)(mod\ 9),$$

assim,

$$3a^2 + 4 \equiv \epsilon\lambda \equiv \pm 1(mod\ 9),$$

dando

$$3a^2 \equiv 4(mod\ 9),\ ou\ 3a^2 \equiv 6(mod\ 9),$$

sendo que ambos são impossíveis de acontecerem.

Caso (ii): $k \equiv 7(mod\ 9)$ e $U \equiv \pm 3(mod\ 9)$. Neste caso, temos $U^2 \equiv 0(mod\ 9)$. Então como $T^2 - kU^2 = 1$ concluímos que $T^2 \equiv 1(mod\ 9)$, e assim

$$T \equiv \epsilon(mod\ 9), \epsilon = \pm 1.$$

Em seguida, de (6.7) módulo 3, obtemos

$$1 \equiv \epsilon b^3(mod\ 3),$$

de modo que

$$b \equiv \epsilon(mod\ 3)\ e\ b^3 \equiv \epsilon(mod\ 9).$$

Então, de (6.7) módulo 9 temos

$$1 \equiv 3a^2 + 7 \pm 3a^3 (mod\ 9).$$

Claramente, isso implica que $a \not\equiv 0(mod\ 3)$, então $a \equiv \pm 1(mod\ 3), a^2 \equiv 1(mod\ 3)$, e $a^3 \equiv a(mod\ 3)$.

Portanto

$$1 \equiv 1 \pm 3a(mod\ 9),$$

dando $a \equiv 0(mod\ 3)$, uma contradição.

Caso (iii): $k \equiv 4(mod\ 7)$ e $U \equiv 0(mod\ 7)$. Para

$$y + \sqrt{k} = (T \pm U\sqrt{k})(a + b\sqrt{k})^3$$

concluímos que

$$y - \sqrt{k} = (T \mp U\sqrt{k})(a - b\sqrt{k})^3,$$

assim,

$$\begin{gathered} x^3 = y^2 - k = (y + \sqrt{k})(y - \sqrt{k}) = \\ = (T \pm U\sqrt{k})(a + b\sqrt{k})^3 (T \mp U\sqrt{k})(a - b\sqrt{k})^3 = \\ = (T^2 - kU^2)(a^2 - kb^2)^3 = (a^2 - kb^2)^3 \end{gathered}$$

e portanto

$$x = a^2 - kb^2.$$

Agora, como

$$x^3 \equiv 0(mod\ 7)\ ou\ x^3 \equiv 1(mod\ 7)\ ou\ x^3 \equiv 6(mod\ 7)$$

e

$$y^2 \equiv 0(mod\ 7)\ ou\ y^2 \equiv 1(mod\ 7)\ ou\ y^2 \equiv 2(mod\ 7)\ ou\ y^2 \equiv 4(mod\ 7),$$

segue que

$$y^2 - x^3 = k \equiv 4(mod\ 7)$$

que dá

$$y^2 \equiv 4(mod\ 7)\ e\ x^3 \equiv 0(mod\ 7).$$

Portanto,

$$x \equiv 0(mod\ 7)$$

e então

$$a^2 - 4b^2 \equiv 0(mod\ 7);$$

isto é,

$$a \equiv \pm 2b(mod\ 7).$$

De $U \equiv 0(mod\ 7)$ e $T^2 - kU^2 = 1$ concluímos

$$T^2 \equiv 1(mod\ 49)$$

assim

$$T \equiv \pm 1(mod\ 49).$$

Então de (6.7) obtemos que

$$1 \equiv \pm 2b^3(mod\ 7),$$

o que é impossível.

Isso completa a demonstração que $y^2 = x^3 + k$ não tem solução nos três casos para $x, y \in \mathbb{Z}$. □

Exemplo 6.4. Escolhendo $k = 58$ temos que $k \equiv 2(mod\ 4)$ e $k \equiv 4(mod\ 9)$. Neste caso, $h(\mathbb{Q}(\sqrt{58})) = 2$ e a unidade fundamental de $\mathbb{Q}(\sqrt{58})$ é

$$99 + 13\sqrt{58}$$

de norma -1. Assim a unidade fundamental de norma 1 é

$$(99 + 13\sqrt{58})^2 = 19603 + 2574\sqrt{58}$$

então

$$U = 2574 \equiv 0(mod\ 9).$$

Portanto, pelo Teorema 6.4, a equação $y^2 = x^3 + 58$ não tem solução em inteiros x e y.

Exemplo 6.5. Escolhendo $k = 7$. Daí $k \equiv 3(mod\ 4)$ e $k \equiv 7(mod\ 9)$. Assim, $h(\mathbb{Q}(\sqrt{7})) = 1$ e a unidade fundamental de $\mathbb{Q}(\sqrt{7})$ de norma 1 é

$$8 + 3\sqrt{7}$$

assim $U = 3 \equiv 3(mod\ 9)$. Logo, pelo Teorema 6.4, a equação $y^2 = x^3 + 7$ não tem solução em inteiros x e y.

Exemplo 6.6. Escolhendo $k = 158$. Daí $k \equiv 2(mod\ 4)$ e $k \equiv 4(mod\ 7)$. Assim, $h(\mathbb{Q}(\sqrt{158})) = 1$ e a unidade fundamental de $\mathbb{Q}(\sqrt{158})$ de norma 1 é

$$7743 + 616\sqrt{158}$$

de modo que $U = 616 \equiv 0(mod\ 7)$. Portanto, pelo Teorema 6.4, a equação $y^2 = x^3 + 158$ não tem solução em inteiros x e y.

Teorema 6.5. *[1] A equação*

$$y^2 = x^3 - 31 \tag{6.9}$$

não tem solução para $x, y \in \mathbb{Z}$.

Demonstração. Suponha que $y^2 = x^3 - 31$ tem uma solução em inteiros x e y.

Primeiramente, note que $31 \nmid y$, pois se $31 \mid y$ então $31 \mid x$ e assim $31^2 \mid x^3 - y^2 = 31$, uma contradição.

Agora vamos mostrar que x é par. Suponha que x é ímpar. Se $x \equiv 1(mod\ 4)$ então $x^3 \equiv 1(mod\ 4)$ e assim $y^2 \equiv 2(mod\ 4)$, o que é impossível. Se $x \equiv 3(mod\ 4)$ então $x^2 + 3x + 9 \equiv 3(mod\ 4)$. Portanto $x^2 + 3x + 9 > 1$.

Daí $x^2 + 3x + 9$ tem um fator primo $p \equiv 3(mod\ 4)$. Agora,

$$y^2 + 4 = x^3 - 27 = (x - 3)(x^2 + 3x + 9),$$

de modo que $y^2 + 4 \equiv 0(mod\ p)$, que é impossível. Isso prova que x é par e y é ímpar.

Uma base integral para $\mathbb{K} = \mathbb{Q}(\sqrt{-31})$ é $\left\{1, \frac{1+\sqrt{-31}}{2}\right\}$. A fatoração em ideal primo de 2 em $\mathcal{O}_{\mathbb{K}}$ é dada por

$$\langle 2 \rangle = \left\langle 2, \frac{3 + \sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{3 - \sqrt{-31}}{2} \right\rangle. \tag{6.10}$$

Mostramos agora que $\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle$ não é um ideal principal. Suponha o contrário, que $\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle$ é um ideal principal. Então existem inteiros a e b tais que

$$\left\langle 2, \frac{3 + \sqrt{-31}}{2} \right\rangle = \left\langle a + b\left(\frac{1 + \sqrt{-31}}{2}\right) \right\rangle.$$

Tomando as normas, obtemos

$$2 = N\left(\left\langle 2, \frac{3 + \sqrt{-31}}{2} \right\rangle\right) = N\left(\left\langle a + b\left(\frac{1 + \sqrt{-31}}{2}\right) \right\rangle\right) =$$
$$\left| N\left(\frac{2a + b + b\sqrt{-31}}{2}\right) \right| = \frac{(2a + b)^2 + 31b^2}{4}$$

assim,

$$(2a + b)^2 + 31b^2 = 8,$$

que é impossível.

Em seguida, aplicando (6.9) e (6.10), concluímos que

$$\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = \left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{y-\sqrt{-31}}{2} \right\rangle \left\langle \frac{x}{2} \right\rangle^3. \tag{6.11}$$

Mostramos agora que os dois ideais $\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle$ e $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$ são primos entre si. Suponhamos que eles não são primos entre si, então existe um ideal primo P tal que

$$P \mid \left\langle \frac{y+\sqrt{-31}}{2} \right\rangle \ e \ P \mid \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle.$$

Então,

$$\frac{y+\sqrt{-31}}{2} \in P \ e \ \frac{y-\sqrt{-31}}{2} \in P,$$

assim

$$\sqrt{-31} = \left(\frac{y+\sqrt{-31}}{2} \right) - \left(\frac{y-\sqrt{-31}}{2} \right) \in P.$$

Portanto,

$$P \mid \left\langle \sqrt{-31} \right\rangle.$$

Mas P e $\left\langle \sqrt{-31} \right\rangle$ ambos são ideais primos de modo que

$$P = \left\langle \sqrt{-31} \right\rangle.$$

Consequentemente,

$$\left\langle \sqrt{-31} \right\rangle \mid \left\langle \left(\frac{y+\sqrt{-31}}{2} \right) \right\rangle$$

de modo que $\frac{y+\sqrt{-31}}{2} \in \left\langle \sqrt{-31} \right\rangle$. Isso mostra que existem inteiros u e v tais que

$$\frac{y+\sqrt{-31}}{2} = \sqrt{-31} \left(\frac{u+v\sqrt{-31}}{2} \right).$$

Daí $u = 1$ e $y = -31v$, contradizendo $31 \nmid y$. Isso prova que os ideais $\left\langle \left(\frac{y+\sqrt{-31}}{2} \right) \right\rangle$ e $\left\langle \left(\frac{y-\sqrt{-31}}{2} \right) \right\rangle$ são primos entre si. Assim, substituindo y por $-y$ se necessário, vemos a partir de (6.11) que existe um ideal A de $\mathcal{O}_{\mathbb{K}}$ tal que

$$\begin{cases} \left\langle \left(\frac{y+\sqrt{-31}}{2} \right) \right\rangle = \left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle A^3, \\ \left\langle \left(\frac{y-\sqrt{-31}}{2} \right) \right\rangle = \left\langle 2, \frac{3-\sqrt{-31}}{2} \right\rangle \overline{A}^3, \\ \left\langle \frac{x}{2} \right\rangle = A\overline{A}, \end{cases} \tag{6.12}$$

onde $\overline{A}$ denota o ideal conjugado de A. Como $h(\mathbb{Q}(\sqrt{-31})) = 3$ o ideal A^3 é principal. Então, a partir da primeira igualdade de (6.12), concluímos que o ideal $\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle$ é principal, uma contradição. Isso completa a demonstração de que a equação $y^2 = x^3 - 31$ não tem solução para $x, y \in \mathbb{Z}$. □

Concluímos essa seção dando duas tabelas (Tabelas (6.1) e (6.2)) de soluções de $y^2 = x^3 + k$ (ver [1]).

Tabela 6.1: Soluções $(x, y) \in \mathbb{Z}^2$ de

$$y^2 = x^3 + k, -20 \leq k < 0$$

k	Soluções (x, y) de $y^2 = x^3 + k$
-1	$(1, 0)$
-2	$(3, \pm 5)$
-3	sem solução
-4	$(2, \pm 2), (5, \pm 11)$
-5	sem solução
-6	sem solução
-7	$(2, \pm 1), (32, \pm 181)$
-8	$(2, 0)$
-9	sem solução
-10	sem solução
-11	$(3, \pm 4), (15, \pm 58)$
-12	sem solução
-13	$(17, \pm 70)$
-14	sem solução
-15	$(4, \pm 7)$
-16	sem solução
-17	sem solução
-18	$(3, \pm 3)$
-19	$(7, \pm 18)$
-20	$(6, \pm 14)$

Tabela 6.2: Soluções $(x, y) \in \mathbb{Z}^2$ de $y^2 = x^3 + k, 0 < k \leq 20$

k	Soluções (x, y) de $y^2 = x^3 + k$
1	$(-1, 0), (0, \pm 1), (2, \pm 3)$
2	$(-1, \pm 1)$
3	$(1, \pm 2)$
4	$(0, \pm 2)$
5	$(-1, \pm 2)$
6	sem solução
7	sem solução
8	$(-2, 0), (1, \pm 3), (2, \pm 4), (46, \pm 312)$
9	$(-2, \pm 1), (0, \pm 3), (3, \pm 6), (6, \pm 15), (40, \pm 253)$
10	$(-1, \pm 3)$
11	sem solução
12	$(-2, \pm 2), (13, \pm 47)$
13	sem solução
14	sem solução
15	$(1, \pm 4), (109, \pm 1138)$
16	$(0, \pm 4)$
17	$(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23), (43, \pm 282), (52, \pm 375), (5234, \pm 378661)$
18	$(7, \pm 19)$
19	$(5, \pm 12)$
20	sem solução

7 Considerações Finais

O presente trabalho foi dedicado ao estudo de teoria dos números algébricos, abordando alguns tópicos e aplicações. A teoria dos números algébricos teve uma grande parte de seu desenvolvimento por meio de tentativas de solução da Equação de Fermat, pois os inteiros algébricos apareceram como ferramenta para tratar esse problema.

Primeiramente, focamos nos tópicos de teoria dos números algébricos, começando com conceitos que servem de base para os estudos mais profundos e resultados importantes para a sequência do trabalho. No entanto, nosso objetivo maior, foi a aplicação em teoria dos números algébricos e devido ao grande número de aplicações foram escolhidas somente duas delas para serem apresentadas.

Uma das aplicações presente no trabalho é a teoria sobre os reticulados. Um reticulado no $\mathbb{R}^n$, intuitivamente, é um conjunto infinito de pontos dispostos de forma regular e os reticulados de maior interesse são aqueles com maior densidade de empacotamento. A construção algébrica de reticulados está diretamente ligada com o anel dos inteiros de um corpo de números e é difícil encontrar esse anel dos inteiros para qualquer corpo, uma vez que o anel dos inteiros de corpos conhecidos são apenas os anéis dos inteiros dos corpos quadráticos e ciclotômicos.

A outra aplicação é sobre as equações Diofantinas. Essas equações possuem coeficientes e soluções inteiras apresentadas geralmente com mais de uma variável, tais soluções existem quando consideramos um domínio euclidiano.

Algumas dessas equações Diofantinas foram estudadas por grandes matemáticos como Fermat, que estudou a equação $x^n + y^n = z^n$. Outra equação que aparece muito nas bibliografias é a equação de Pell $x^2 - dy^2 = 1$. Já a equação Diofantina que foi abordada neste trabalho é a equação $y^2 = x^3 + k$, que muitas vezes é chamada de equação de Bachet. O maior problema de verificar se uma equação é Diofantina reside no fato de que muitas vezes uma equação não possui solução somente nos inteiros. Vimos que o número de classe de $\mathbb{K} = \mathbb{Q}(\sqrt{k})$ está relacionado com as soluções da equação $y^2 = x^3 + k$ e para encontrá-las analisamos o caso em que k é positivo ou negativo.

Por fim, vale ressaltar que ainda há muitos resultados que podem ser obtidos utilizando esta teoria e muitas aplicações a serem estudadas partindo dos resultados deste trabalho.

Referências

[1] ALACA, S.; WILLIAMS, K.S. *Introductory Algebraic Number Theory.* Cambridge University Press, New York, 2004.

[2] CRAIG, M. *Extreme Forms and Cyclotomy.* Math. 25, pp. 44-56, 1978.

[3] FLORES, A. L.; INTERLANDO, J. C.; NETO, T. P. N.; CONTIERO, A. L. *A new number field construction of the lattice* E_8. Beitrage zur Algebra und Geometrie , vol. 54, Issue 2, pp. 503-508, 2013.

[4] HERSTEIN, I. N. *Topics in Algebra.* John Wiley & Sons, New York, 1975.

[5] HOFFMAN, K.; KUNZE, R. *Álgebra Linear.* Editora Polígono S. A., São Paulo, 1971.

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

[7] MARCUS, D. A. *Numbers Fields.* Springer-Verlag, 1977.

[8] MOLLIN, R. A. *Algebraic Number Theory.* CRC Press, University of Calgary, Alberta, Canada, 2011.

[9] OGGIER, F. *Algebraic Methods for Channel Coding.* 2005, 125f. Tese (Doutorado em Matemática e Informática), École Polytechnique Fédeérale de Lausanne, Lausane, 2005.

[10] RIBEIRO, A. C. *Reticulados sobre Corpos de Números.* Dissertação de Mestrado, IBILCE-UNESP, São José do Rio Preto, 2003.

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

[12] SANTOS, J. P. O. *Introdução à Teoria dos Números.* IMPA, Rio de Janeiro, 1998.

[13] SLOANE, N. J. A.; CONWAY, J. H. *Sphere Packing, Lattices and Groups.* Springer-Verlag, 1999.

[14] STEIN, W. *Algebraic Number Theory, a Computational Approach.* Harvard, Massachusetts, 2012.

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

[16] STEWART, I. N. *Galois Theory.* Chapman and Hall/CRC, Conventry, 2003.

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