

Andréia Cristina Ribeiro

Reticulados sobre Corpos de Números



1910001192



Reticulados sobre Corpos de Números

Andréia Cristina Ribeiro

Orientador: Prof. Dr. Antonio Aparecido de Andrade

Dissertação apresentada ao Departamento
de Matemática - IBILCE - UNESP, como
parte dos requisitos para a obtenção do
Título de Mestre em Ciências Matemáticas
- Área de Concentração: Matemática.



t. 1.192/03

Fevereiro - 2003
São José do Rio Preto - SP

“ Há duas fontes perenes de alegria pura:
o bem realizado e o dever cumprido.”

Eduardo Girão



Agradecimentos

A todos os que me ajudaram, agradeço.

A Deus

Ao Prof. Dr. Antônio Aparecido de Andrade, pela amizade tão sincera, pela paciência, dedicação e desprendimento durante a minha orientação.

Aos professores do Departamento de Matemática da UNESP-S.J.R. Paulo, pela excelente formação e amizade.

Aos professores da base de engenharia: Prof. Dr. Epitácio A. F. de Oliveira (FEF-Prém), Elina Belloso, Prof. Dr. Eduardo L. C. Faria (MIL-Prém), S.J.R. Paulo, Prof. Dr. Henrique Lázaro (MIL-Prém), Ruy Chaves e Prof. Dr. Gregório P. S. Leite (MIL-Prém), S.J.R. Paulo.

Aos colegas, pela ajuda e apoio, especialmente à parte de matemática, durante o trabalho.

Aos meus colegas do curso de Engenharia, em particular a Ilaciana, Flávia e Tatiana, pela amizade sincera.

A minha mãe, a Sr. Tatiana, por proporcionar os estudos, trabalho e dedicação durante os meus estudos, que me possibilitou.

Aos meus pais, Marcelino e Clotilde, pela amor e incentivo durante toda a minha vida acadêmica.

Ao meu pai, a Sr. Tatiana, pela orientação, incentivo e por ter sido o meu primeiro professor.

Ao meu esposo Aparecido Clarete,
à minha filha Renata
e à minha irmã Joana D'arc
(in memoriam)

dedico.

Aos meus amigos, pela ajuda e apoio durante o trabalho.

A minha amiga Ellen, pela ajuda e apoio durante o trabalho.

A FAPESP pelo auxílio financeiro.

A todos que durante os estudos, proporcionaram a minha formação acadêmica.

Agradecimentos

Ao concluir este trabalho, agradeço:

A Deus.

Ao Prof. Dr. Antonio Aparecido de Andrade, pela amizade tão sincera, pela paciência, dedicação e desprendimento durante a valiosa orientação.

Aos professores do Departamento de Matemática da UNESP-S.J.R.Preto, pela excelente formação e amizade.

Aos professores da banca examinadora: Prof^a Dr^a Roseli A. F. de Oliveira (FEIS-Unesp, Ilha Solteira), Prof^a Dr^a Ermínia L. C. Fanti (IBILCE-Unesp, S.J.R.Preto), Prof. Dr. Henrique Lázari (IGCE-Unesp, Rio Claro) e Prof. Dr. Trajano P. N. Neto (IBILCE-Unesp, S.J.R.Preto).

Ao Márcio, pela disponibilidade dispensada à parte ilustrativa deste trabalho.

Aos meus colegas do curso de Pós-graduação, em particular, à Barbara, Flávia e TatiMi, pelo agradável convívio.

À minha grande amiga TatiB por compartilhar as alegrias, tristezas e dificuldades durante nossa caminhada que ora completamos.

Aos meus pais Durvalino e Floriza, pelo amor e incentivo inestimado que sempre me transmitiram.

Ao meu esposo Clarete, pelo carinho, confiança e por me apoiar principalmente nos momentos difíceis.

À minha querida filha Renata pela sua compreensão e pelo seu amor.

Ao meu sogro Aparecido e minha sogra Rita, pelo apoio e cuidados com a Renata.

Ao meu tio Salvador, por todos os bons conselhos dados durante toda a minha vida.

À minha amiga Ellen, pela agradável companhia e pela sua amizade.

À FAPESP pelo auxílio financeiro.

A todos que direta ou indiretamente contribuíram para a realização deste trabalho.



Resumo

O principal objetivo do presente trabalho é o estudo de reticulados no $\mathbb{R}^n$ via o homomorfismo de Minkowski. Deste modo, dado um ideal $\mathfrak{a}$ do anel dos inteiros algébricos de um corpo numérico, tem-se que a imagem deste ideal via o homomorfismo de Minkowski é um reticulado no $\mathbb{R}^n$. Como casos particulares estudamos os reticulados obtidos das extensões $\mathbb{Q}(\sqrt[n]{d})$, $n = 2, 3, 4, 5$, com d um inteiro livre de quadrados.

Palavras-chave: reticulados, densidade de empacotamento, densidade de centro e empacotamento esférico.



Abstract

The main goal of this work is the study of lattices in $\mathbb{R}^n$ through the Minkowski homomorphism. We established that the image of an ideal $\mathfrak{a}$ of the algebraic integer ring of a number field by the Minkowski homomorphism is a lattice in $\mathbb{R}^n$. As a particular case we study the lattices obtained from the extensions $\mathbb{Q}(\sqrt[n]{d})$, $n = 2, 3, 4, 5$, where d is an integer free of square power.

Keywords: lattices, density of packing, density of center and sphere packing.

Conteúdo

Introdução	vii
1 Preliminares	1
1.1 Álgebra abstrata	1
2 Teoria Algébrica dos Números	7
2.1 Elementos inteiros sobre um anel	7
2.2 Elementos algébricos sobre um corpo e extensões algébricas	11
2.3 Norma e traço em uma extensão	15
2.4 Discriminante	18
2.5 Corpos ciclotômicos	23
2.6 Anéis Noetherianos	26
2.7 Anéis de Dedekind	29
2.8 Norma de um ideal	33
2.9 Fatoração de um ideal em uma extensão	36
2.10 Discriminante e ramificação	46
3 Reticulados	53
3.1 Reticulados	53
3.2 Empacotamento esférico	60
3.3 Reticulados importantes e suas propriedades	62
3.4 Homomorfismo canônico de um corpo de números	64



4

Aplicações no $\mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^4$ e $\mathbb{R}^5$

72

4.1

Reticulados em corpos quadráticos

73

4.2

Reticulados nas Cúbicas

75

4.3

Reticulados nas Quárticas

77

4.4

Reticulados nas Quínticas

80

Bibliografia

85



Introdução

Empacotamento esférico é a disposição de esferas de mesmo raio no espaço euclidiano n -dimensional de tal modo que a intersecção de duas delas tenha no máximo um ponto. O objetivo do empacotamento é encontrar um arranjo de esferas idênticas de tal forma que a fração do espaço coberto por essas esferas seja o maior possível.

A forma de dispor essas esferas de modo a cobrir a maior parte do espaço, tem sido um desafio e merece a citação de Hilbert em 1900 com o 18º Problema de uma lista de desafios que ocuparam destaque no desenvolvimento da ciência. Assim, muitas teorias evoluíram tendo o 18º Problema de Hilbert com ponto de partida, descrevendo vários modelos matemáticos com a finalidade de obter empacotamento esférico com alta densidade, onde foram obtidas algumas cotas.

Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis. Os empacotamentos esféricos, tal que o conjunto de centros das esferas constituem um subgrupo discreto do espaço euclidiano despertaram interesse e passaram a ser chamados de empacotamentos reticulados, onde a teoria de $\mathbb{Z}$ -módulos passou a ser muito utilizada no sentido de obter melhores reticulados e que em grande parte das dimensões os empacotamentos esféricos mais densos são os empacotamentos reticulados.

Em 1948 com a publicação do artigo de Shannon, onde ficou estabelecida uma estreita relação entre códigos com alto desempenho e empacotamentos reticulados densos, o interesse pelo 18º Problema de Hilbert aumentou consideravelmente, com o surgimento de várias famílias de reticulados, cada uma destas se propondo a dar a melhor contribuição no que diz respeito a densidade de empacotamento.

Dentre tais modelos destaca-se o descrito por Minkowski, no final do século XIX / início



do século XX. Nesta época Minkowski estava interessado em provar a finitude do Grupo de Classes, quando desenvolvia a sua teoria de Corpos de Classes.

Tal modelo consiste de um corpo de números K de grau n e o seu anel de inteiros algébricos $\mathcal{O}_K$, de onde obtém-se um homomorfismo de K em $\mathbb{R}^n$, com o auxílio dos n monomorfismos de K em $\mathbb{C}$, de modo que a imagem de um ideal ordinário não nulo de $\mathcal{O}_K$ é um reticulado de posto n em $\mathbb{R}^n$.

O cálculo da densidade de centro de tal reticulado é feito a partir do discriminante do corpo, da norma do ideal e da minimização de uma forma quadrática com entradas inteiras originada da função traço. Como podemos ver, o problema de empacotamento reticulado, via o modelo de Minkowski, encontrou na Teoria Algébrica dos Números ferramentas que viabilizaram o efetivo cálculo da densidade de centro.

Desta maneira o presente trabalho tem por objetivo estudar os reticulados no $\mathbb{R}^n$ obtidos via o método de Minkowski (homomorfismo canônico), enfocando os seus principais parâmetros tais como região fundamental, empacotamento esférico, densidade de empacotamento e densidade de centro. Para tanto o trabalho se divide da seguinte maneira.

No Capítulo 1 recordamos em linhas gerais os conceitos básicos da álgebra abstrata.

No Capítulo 2, fazendo uso das referências [2], [4] e [6], apresentamos um estudo completo sobre teoria algébrica dos números, onde vemos elementos inteiros sobre um anel, elementos algébricos sobre um corpo e extensões algébricas, norma e traço de elementos, discriminante, corpos ciclotômicos, anéis Noetherianos, Anéis de Dedekind, norma de ideal e sua fatoração em uma extensão.

No Capítulo 3 fazemos o estudo de reticulados no $\mathbb{R}^n$ enfocando os seus principais parâmetros tais como região fundamental, empacotamento esférico, densidade de empacotamento e densidade de centro. Além disso, apresentamos vários reticulados construtivos com o intuito de ressaltar a existência de reticulados que não são obtidos via o método de Minkowski e então veremos o homomorfismo canônico de um corpo de números, e a partir dele obteremos reticulados no $\mathbb{R}^n$ via o anel dos inteiros do corpo de números, onde determinamos os volumes dos reticulados obtidos via o homomorfismo canônico, tendo como base as referências [1], [2] e [4].

No Capítulo 4 daremos aplicações da teoria apresentada nos capítulos anteriores, mais



precisamente, calculamos a densidade de centro de alguns reticulados obtidos via o homomorfismo canônico. Nosso maior desafio no cálculo efetivo da densidade de centro é minimizar uma forma quadrática, caracterizada em função do traço relativo. No caso dos corpos quadráticos caracterizamos a forma quadrática e calculamos a densidade de centro da realização geométrica do anel dos inteiros algébricos e de ideais principais. No estudo das cúbicas [7], quárticas [5] e quánticas, restringimo-nos à aquelas da forma $\mathbb{Q}(\sqrt[3]{d})$, $\mathbb{Q}(\sqrt[4]{d})$ e $\mathbb{Q}(\sqrt[5]{d})$, com d um inteiro livre de quadrados. Sob tais condições caracterizamos o anel dos inteiros algébricos e sua forma quadrática. O valor mínimo da forma quadrática é obtido atribuindo valores inteiros às variáveis e comparando os resultados. No caso de um ideal do anel dos inteiros algébricos de $\mathbb{Q}(\sqrt[3]{d})$, $\mathbb{Q}(\sqrt[4]{d})$ e $\mathbb{Q}(\sqrt[5]{d})$ a forma quadrática é minimizada com valores inteiros e ainda satisfazendo condições que caracterizam os elementos do ideal. O Lema de Kummer 2.9.3 é de fundamental importância neste contexto. Com este resultado podemos descrever os geradores de ideais primos e obter o grau residual e o índice de ramificação.

1.1 Álgebra abstrata



Capítulo 1

Preliminares

Neste Capítulo faremos uma revisão de álgebra abstrata necessária para o entendimento do restante do nosso trabalho.

1.1 Álgebra abstrata

Iniciaremos esta seção relembrando alguns conceitos básicos de álgebra, e a seguir daremos resultados de grande importância para a compreensão do próximo capítulo sobre teoria algébrica dos números.

Um **anel** $\langle A, +, \cdot \rangle$ é um conjunto A munido de duas operações binárias $+$ e $\cdot$, as quais chamamos adição e multiplicação, tal que A com a adição é um grupo abeliano, a multiplicação é associativa e satisfaz a lei distributiva da multiplicação em relação a adição. Como exemplos de anéis podemos citar o conjunto dos números inteiros sob adição e multiplicação, o conjunto $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ sob as operações de soma e produto módulo n , os polinômios da forma $a_0 + a_1X + a_2X^2 + \dots + a_nX^n$ na indeterminada X e a_i 's coeficientes inteiros. Dado $N \subseteq A$ não vazio, dizemos que N é um **subanel** de um anel A se N também for um anel com as operações de adição e multiplicação herdadas de A . Um **anel comutativo com unidade** é um anel cuja a multiplicação é comutativa e existe o elemento neutro da multiplicação chamado de unidade do anel. Ao longo de nosso trabalho, um anel será sempre comutativo com unidade. Um elemento não nulo a de A é denominado **divisor de zero** se existe um elemento não nulo b em A tal que $a \cdot b = 0$ ou $b \cdot a = 0$. Se A for um anel



A for um anel com unidade, um elemento a de A é denominado **invertível** em A se existir a^{-1} em A tal que $a.a^{-1} = a^{-1}.a = 1$. O conjunto dos elementos invertíveis de A é um grupo multiplicativo que será denotado por A^* . Um anel A , comutativo com unidade, que satisfaz a lei do anulamento do produto, ou seja, se $ab = 0$ com $a, b \in A$, então $a = 0$ ou $b = 0$, recebe o nome de **anel de integridade**, também chamado de **domínio**.

Seja A um anel comutativo e seja $\mathfrak{a} \neq \emptyset$ um subconjunto de A . Dizemos que $\mathfrak{a}$ é um ideal em A se, e somente se, $\forall x, y \in \mathfrak{a} \implies x - y \in \mathfrak{a}$, e $\forall a \in A, x \in \mathfrak{a}$, tal que $ax \in \mathfrak{a}$. Os conjuntos $\{0\}$ e A são ideais de A , chamados ideais triviais de A , e os ideais não triviais de A são chamados ideais próprios de A . O ideal $\langle a_1, a_2, \dots, a_n \rangle = \{x_1a_1 + x_2a_2 + \dots + x_na_n \mid x_i \in A\}$ de A é chamado **ideal gerado** por $a_1, a_2, \dots, a_n$. Um ideal gerado por um só elemento $a \in A$ recebe o nome de **ideal principal gerado por a** . Neste caso, além da notação $\langle a \rangle$, também é comum usarmos a notação aA . Se todos os ideais de um anel são principais, então este anel é chamado de **anel principal**. Por exemplo, se $\mathfrak{a}$ é um ideal em $\mathbb{Z}$, então existe $n \in \mathbb{Z}$ de tal modo que $\mathfrak{a} = n\mathbb{Z}$, ou seja, $\mathbb{Z}$ é um anel principal. Dado $\mathfrak{p}$ um ideal em um anel A , dizemos que $\mathfrak{p}$ é um **ideal primo** se $\mathfrak{p} \neq A$ e se é satisfeita a seguinte sentença: $(\forall a, b \in A)(a.b \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p})$. Um ideal $\mathfrak{m}$ em um anel A é dito um **ideal maximal** se $\mathfrak{m} \neq A$, e satisfaz a seguinte propriedade: $\mathfrak{m}$ é o elemento maximal em relação à inclusão, no conjunto dos ideais em A que são diferentes de A , ou seja, se existir um ideal $\mathfrak{a}$ do anel A tal que $\mathfrak{m} \subset \mathfrak{a} \subset A \implies \mathfrak{m} = \mathfrak{a}$ ou $\mathfrak{a} = A$. Por exemplo, se considerarmos $A = \mathbb{Z}$ e p um número primo de $\mathbb{Z}$, temos que $\langle p \rangle$ é um ideal primo e também é um ideal maximal. Dado A um anel comutativo com unidade, temos que todo ideal maximal em A é primo e se A for um domínio principal e $\mathfrak{p} \neq 0$ for um ideal primo, segue que, $\mathfrak{p}$ é maximal.

Sejam A um anel, $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A . Definimos a soma dos ideais $\mathfrak{a}$ e $\mathfrak{b}$ como $\mathfrak{a} + \mathfrak{b} = \{x + y; x \in \mathfrak{a} \text{ e } y \in \mathfrak{b}\}$, que também é um ideal de A . Também definimos o produto de $\mathfrak{a}$ e $\mathfrak{b}$ como $\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^n x_i y_i; x_i \in \mathfrak{a} \text{ e } y_i \in \mathfrak{b} \right\}$, que também é um ideal de A . Dizemos que os ideais $\mathfrak{a}$ e $\mathfrak{b}$ são **comaximais** se $\mathfrak{a} + \mathfrak{b} = A$.

Um anel A , comutativo com unidade, recebe o nome de **corpo** se todo elemento não nulo de A admite simétrico multiplicativo, ou seja, todo elemento não nulo de A é invertível, e denotaremos esse corpo por K . Se K é corpo, então temos que $\{0\}$ é um ideal maximal em K e os únicos ideais de K são os triviais. Um subconjunto $L \subset K$ é um **subcorpo** de K se

$\mathbb{L}$ também for um corpo com as operações de soma e produto herdadas de $\mathbb{K}$. Neste caso, dizemos que $\mathbb{K}$ é uma extensão de $\mathbb{L}$.

Seja $A[X]$ o conjunto de todos os polinômios na variável X , sobre um anel A , temos que $A[X]$ é um anel com as operações de adição e multiplicação de polinômios, chamado **anel de polinômios**. Se A for um domínio, então $A[X]$ também será, se $\mathbb{K}$ for corpo, então todo ideal em $\mathbb{K}[X]$ será principal, ou seja, $\mathbb{K}[X]$ é principal.

Dado um domínio A , o seu **corpo de frações** é o conjunto $\mathbb{K} = \left\{ \frac{a}{b}, \text{ com } a, b \in A \text{ e } b \neq 0 \right\}$.

Sejam A um anel comutativo e $\mathfrak{a} \subset A$ um ideal. Dado $x \in A$, o conjunto $x + \mathfrak{a} = \{x + y; y \in \mathfrak{a}\}$ é chamado de **classe lateral** de $\mathfrak{a}$. Definindo a soma $(x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a}$ e o produto $(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$, para todo $x, y \in A$, temos que o conjunto de todas as classes laterais de $\mathfrak{a}$ é um anel, chamado de **anel quociente** e denotado por $A/\mathfrak{a}$.

Temos que $\mathfrak{p}$ é um ideal primo de um anel A se, e somente se, o anel quociente $A/\mathfrak{p}$ é um domínio, e que $\mathfrak{m}$ é um ideal maximal de A se, e somente se, o anel quociente $A/\mathfrak{m}$ é um corpo. Se A e B são anéis, dizemos que uma aplicação $f : A \rightarrow B$ é um **homomorfismo de anéis** se, $\forall x, y \in A$ tem-se, $f(x + y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$. Se, além disso, f for bijetora, a aplicação f é denominada de **isomorfismo**, e usamos a seguinte notação, $A \simeq B$, e se $A = B$ temos que a aplicação f é um **automorfismo**.

Segue da definição de homomorfismo de anéis que $f(-a) = -f(a)$, $f(0_A) = 0_B$ e que $f(na) = nf(a)$, $\forall a \in A$ e $\forall n \in \mathbb{Z}$, onde 0_A é o zero de A e 0_B é o zero de B . O núcleo da aplicação f é definido por $\text{Ker}(f) = \{x \in A \mid f(x) = 0_B\}$, e a imagem da aplicação f por $\text{Im}(f) = \{f(x) \mid x \in A\}$. Temos que o $\text{Ker}(f)$ é um ideal de A , e que a $\text{Im}(f)$ é um subanel de B .

Teorema 1.1.1 (Teorema do Isomorfismo para Anéis) *Sejam A, B anéis e seja $f : A \rightarrow B$ um homomorfismo de anéis. Então, $\frac{A}{\text{Ker}(f)} \simeq \text{Im}(f)$.* $\blacksquare$

Proposição 1.1.1 *Sejam A um anel, $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A tais que $\mathfrak{a} + \mathfrak{b} = A$. Então, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ e o homomorfismo canônico $\varphi : A \rightarrow \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}}$ induz o isomorfismo $\theta : \frac{A}{\mathfrak{ab}} \rightarrow \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}}$.*

Demonstração: Temos que $\mathfrak{ab} \subset \mathfrak{a}$ e $\mathfrak{ab} \subset \mathfrak{b}$, e portanto, $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Agora, se $x \in \mathfrak{a} \cap \mathfrak{b}$, como por hipótese $\mathfrak{a} + \mathfrak{b} = A$, então existem elementos $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ tal que $1 = a + b$. Assim, $x = ax + bx$ é a soma de dois elementos de $\mathfrak{ab}$, logo $x \in \mathfrak{ab}$, e portanto, $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. Para o

isomorfismo consideremos $\varphi: A \rightarrow \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}}$, definido por $\varphi(a) = (a + \mathfrak{a}, a + \mathfrak{b})$, com $a \in A$. Assim,

- $\text{Ker}(\varphi) = \mathfrak{a} \cap \mathfrak{b}$. De fato, $x \in \text{Ker}(\varphi) \iff \varphi(x) = (\bar{0}, \bar{0}) \iff (x + \mathfrak{a}, x + \mathfrak{b}) = (\bar{0}, \bar{0}) \iff x + \mathfrak{a} = \bar{0} \text{ e } x + \mathfrak{b} = \bar{0} \iff x \in \mathfrak{a} \text{ e } x \in \mathfrak{b} \iff x \in \mathfrak{a} \cap \mathfrak{b}$.
- φ é sobrejetora. De fato, tomando $(y + \mathfrak{a}, z + \mathfrak{b}) \in \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}}$, temos que encontrar $x \in A$ tal que $(y + \mathfrak{a}, z + \mathfrak{b}) = (x + \mathfrak{a}, x + \mathfrak{b}) = \varphi(x)$. Como $\mathfrak{a} + \mathfrak{b} = A$, temos que $1 = a + b$, com $a \in \mathfrak{a}$ e $b \in \mathfrak{b}$. Tomando $x = az + by$, como $b \equiv 1 \pmod{\mathfrak{a}} \Rightarrow x \equiv y \pmod{\mathfrak{a}}$ e $a \equiv 1 \pmod{\mathfrak{b}} \Rightarrow x \equiv z \pmod{\mathfrak{b}}$, segue que, $x + \mathfrak{a} = y + \mathfrak{a}$ e $x + \mathfrak{b} = z + \mathfrak{b}$.

Portanto, pelo Teorema 1.1.1 temos, $\frac{A}{\mathfrak{a} \cap \mathfrak{b}} \simeq \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}} \xrightarrow{\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}} \frac{A}{\mathfrak{ab}} \simeq \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}}$. ▀

Proposição 1.1.2 *Sejam A um anel e $(\mathfrak{a}_i)_{1 \leq i \leq r}$ um conjunto finito de ideais de A , tais que $\mathfrak{a}_i + \mathfrak{a}_j = A$ para $i \neq j$. Então existe um isomorfismo canônico de $A/\mathfrak{a}_1 \cdots \mathfrak{a}_r$ em $\prod_{i=1}^r A/\mathfrak{a}_i$.*

Demonstração: Faremos a prova por indução sobre r . Da Proposição 1.1.1, o resultado segue para $r = 2$. Agora supomos que o resultado é verdadeiro para todo $k < r$. Fazendo $\mathfrak{b} = \mathfrak{a}_2 \cdots \mathfrak{a}_r$, temos que $\mathfrak{a}_1 + \mathfrak{b} = A$ uma vez que $\mathfrak{a}_1 + \mathfrak{a}_i = A$, para $i \geq 2$. Assim, existem elementos $c_i \in \mathfrak{a}_1$ e $a_i \in \mathfrak{a}_i$ tal que $c_i + a_i = 1$. Logo, $1 = \prod_{i=2}^r (c_i + a_i) = c + a_2 \cdots a_r$, onde c é a soma dos termos que contêm no mínimo um c_i como fator. Portanto, $c \in \mathfrak{a}_1$. Como $\mathfrak{a}_2 \cdots \mathfrak{a}_r \in \mathfrak{b}$, segue que, $\mathfrak{a}_1 + \mathfrak{b} = A$. Pela Proposição 1.1.1, segue que $A/\mathfrak{a}_1 \mathfrak{b}$ é isomorfo a $A/\mathfrak{a}_1 \times A/\mathfrak{b}$, e usando a hipótese de indução temos que $A/\mathfrak{b} = A/\mathfrak{a}_2 \cdots \mathfrak{a}_r$ é isomorfo a $A/\mathfrak{a}_2 \times \cdots \times A/\mathfrak{a}_r$. Portanto, $A/\mathfrak{a}_1 \cdots \mathfrak{a}_r$ é isomorfo à $\prod_{i=1}^r A/\mathfrak{a}_i$. ▀

A seguir veremos o conceito de módulos, enfocando seus principais resultados que serão de grande utilidade para o bom desempenho do prosseguimento do nosso trabalho.

Definição 1.1.1 *Seja A um anel. Um módulo sobre A , ou um A -módulo é um grupo abeliano aditivo M junto com a função $\mu: A \times M \rightarrow M$, denotada por $\mu(a, m) = am$, com $a \in A$ e $m \in M$, que satisfaz as seguintes condições:*

M1) μ é bi-linear, isto é, $\forall \alpha, \beta \in A$ e $\forall m, n \in M$, tem-se que

$$\mu(\alpha + \beta, m) = \mu(\alpha, m) + \mu(\beta, m) \text{ e } \mu(\alpha, m + n) = \mu(\alpha, m) + \mu(\alpha, n),$$

M2) $\mu[(\alpha, \mu(\beta, m))] = \mu(\alpha\beta, m)$, $\forall \alpha, \beta \in A$ e $\forall m \in M$.

M3) $\mu(1, m) = m$, $\forall m \in M$.



A função μ definida acima é chamada de multiplicação escalar do módulo M . Para cada $\alpha \in A$ e cada $m \in M$, o elemento $\mu(\alpha, m) = \alpha m$ de M é chamado de produto por escalar de m por α .

Como exemplos de módulos temos os espaços vetoriais, os anéis sobre si mesmos, os grupos abelianos (como $\mathbb{Z}$ -módulo).

Sejam A um anel e M um A -módulo. Um subconjunto $N \neq \emptyset$ de M é um **submódulo** de M se N é um subgrupo do grupo abeliano aditivo M e conserva a multiplicação escalar de M , isto é, $\alpha x \in N$, $\forall x \in N$ e $\forall \alpha \in A$.

Se um A -módulo M possui um número finito de geradores, dizemos que M é finitamente gerado ou do tipo finito. Se um A -módulo M possui uma base dizemos que M é um **A -módulo livre**, e o número de geradores da base é chamado de posto de M . Observamos que nem todo A -módulo possui uma base.

Lema 1.1.1 *Se T é um conjunto parcialmente ordenado, então as seguintes condições são equivalentes:*

- (a) *Todo subconjunto não vazio de T contém um elemento maximal.*
- (b) *Toda seqüência crescente $(t_n)_{n \geq 0}$ de elementos de T é estacionária.*

Demonstração: Para provarmos $(a) \Rightarrow (b)$, seja t_q um elemento maximal da seqüência crescente (t_n) . Então para $n \geq q$ temos que $t_n = t_q$, ou seja, (t_n) é estacionária. Agora mostremos que $(b) \Rightarrow (a)$. Suponhamos que exista um subconjunto S de T que não possui um elemento maximal. Então para cada $x \in S$, o conjunto dos elementos de S que são maiores do que x é um conjunto não vazio. Pelo axioma da escolha existe uma aplicação $f : S \rightarrow S$ tal que $f(x) > x$ para todo $x \in S$. Como S não é vazio, podemos escolher $t_0 \in S$ e definir por recorrência a seqüência $(t_n)_{n \geq 0}$, onde $t_{n+1} = f(t_n)$. Essa seqüência é estritamente crescente, logo não é estacionária, o que contradiz (b), portanto o conjunto S é vazio. ■

Teorema 1.1.2 *Se A é um anel e M um A -módulo, então as seguintes sentenças são equivalentes.*

- (a) *Toda família não vazia de submódulos de M tem um elemento maximal, considerando a relação de inclusão.*



(b) Toda seqüência crescente $(M_n)_{n \in \mathbb{N}}$ de submódulos de M é estacionária, considerando a relação de inclusão.

(c) Todo submódulo de M é finitamente gerado.

Demonstração: Mostremos que $(a) \Rightarrow (c)$. Sejam N um submódulo de M e Φ o conjunto de todos os submódulos finitamente gerados de N . Temos que Φ é não vazio pois $(0) \in \Phi$. Agora por (a) temos que Φ possui um elemento maximal F . Para $x \in N$, temos que $F + Ax$ é um submódulo finitamente gerado de N , e assim $F + Ax = F$, pois $F + Ax \supset F$ e F é maximal. Portanto, $x \in F$, o que prova que $N \subset F$. Logo $N = F$, e portanto N é finitamente gerado. Provemos agora que $(c) \Rightarrow (b)$. Para isto seja $(M_n)_{n \geq 0}$ uma seqüência crescente de submódulos de M . Temos que $E = \bigcup_{n \geq 0} M_n$ é um submódulo de M , e por (c) temos que E possui um número finito de geradores $\{x_1, \dots, x_q\}$. Como $\{x_1, \dots, x_q\} \subset E$, para todo i existe um índice $n(i)$ tal que $x_i \in M_{n(i)}$. Seja n_0 o maior dos $n(i)$'s. Como (M_n) é crescente, então $x_i \in M_{n_0}$ para todo i , e assim $E \subset M_{n_0}$ e portanto $E = M_{n_0}$, para $n \geq n_0$. Portanto, a seqüência (M_n) é estacionária para $n \geq n_0$. A equivalência de (a) e (b) segue do Lema 1.1.1. $\blacksquare$

Corolário 1.1.1 Em um anel principal A , toda família não vazia de ideais possui um elemento maximal.

Demonstração: Considerando A como um módulo sobre si mesmo, seus submódulos são seus ideais, e como todos os ideais são principais estes são A -módulos gerados por um elemento, ou seja, são finitamente gerados. Assim o resultado segue da implicação $(c) \Rightarrow (a)$ do Teorema 1.1.2. $\blacksquare$

Teorema 1.1.3 [3] Sejam A um anel principal, M um A -módulo livre de posto n , e M' um submódulo de M . Então:

(a) M' é livre de posto q , $0 \leq q \leq n$.

(b) Se $M' \neq 0$, então existe uma base $\{e_1, \dots, e_n\}$ de M e elementos não nulos $a_1, \dots, a_q \in A$ tais que $\{a_1 e_1, \dots, a_q e_q\}$ é uma base de M' e tal que a_i divide a_{i+1} , $1 \leq i \leq q-1$.

Corolário 1.1.2 Sejam A um anel principal e M um A -módulo finitamente gerado. Então M é isomorfo a um produto $(A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \dots \times (A/\mathfrak{a}_n)$, onde os $\mathfrak{a}_i$'s, para $i = 1, \dots, n$, são ideais de A tais que $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \dots \supset \mathfrak{a}_n$.

Capítulo 2

Teoria Algébrica dos Números

Neste capítulo faremos o estudo da teoria algébrica dos números, enfocando elementos inteiros sobre um anel, norma e traço de elementos e de ideais, discriminante, anéis Noetherianos, anéis de Dedekind, fatoração de ideais e ramificação.

2.1 Elementos inteiros sobre um anel

Sejam A um anel e B um subanel de A . Dizemos que um elemento x de A é **inteiro** sobre B se x é raiz de um polinômio mônico com coeficientes em B , ou seja, existem $b_0, \dots, b_{n-1} \in B$ tal que $X^n + b_{n-1}X^{n-1} + \dots + b_1X + b_0 = 0$. Essa equação é chamada de **equação de dependência inteira**.

Exemplo 2.1.1 O elemento $x = \sqrt{2} + \sqrt{3}$ de $\mathbb{R}$ é inteiro sobre $\mathbb{Z}$, pois x é raiz do polinômio $X^4 - 10X^2 + 1 \in \mathbb{Z}[X]$. O elemento $x = \sqrt{2}$ de $\mathbb{R}$ é inteiro sobre $\mathbb{Z}$, pois x é raiz do polinômio $X^2 - 2 \in \mathbb{Z}[X]$. ▀

Teorema 2.1.1 Sejam A um anel, B um subanel de A e $x \in A$. Então as seguintes condições são equivalentes:

- (a) x é inteiro sobre B .
- (b) O anel $B[x]$ é um B -módulo finitamente gerado.
- (c) Existe um subanel R do anel A tal que R é um B -módulo finitamente gerado contendo B e o elemento x .



Demonstração: (a) $\Rightarrow$ (b) Como x é inteiro sobre B , então existem $b_0, \dots, b_{n-1} \in B$ tal que $x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$. Assim, $x^n = -(b_{n-1}x^{n-1} + \dots + b_1x + b_0)$, ou seja, $x^n \in \langle 1, x, \dots, x^{n-1} \rangle$. Vamos mostrar por indução que $x^j \in \langle 1, x, \dots, x^{n-1} \rangle$, para todo $j \in \mathbb{N}$. Temos que $x^j \in \langle 1, x, \dots, x^{n-1} \rangle$ para todo $j \leq n$. Suponhamos que $x^j \in \langle 1, x, \dots, x^{n-1} \rangle$ e mostremos que $x^{j+1} \in \langle 1, x, \dots, x^{n-1} \rangle$. Por hipótese de indução, existem $a_0, \dots, a_{n-1} \in A$, tal que $x^j = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$. Assim, $x^{j+1} = x^jx = (a_0 + a_1x + \dots + a_{n-1}x^{n-1})x = a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} + a_{n-1}x^n = a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1} + a_{n-1}(-b_{n-1}x^{n-1} - \dots - b_1x + b_0) = -a_{n-1}b_0 + (a_0 - b_1)x + \dots + (a_{n-2} - b_{n-1})x^{n-1}$, ou seja, $x^{j+1} \in \langle 1, x, \dots, x^{n-1} \rangle$. Portanto, $x^j \in \langle 1, x, \dots, x^{n-1} \rangle$ para todo $j \in \mathbb{N}$. Agora, como $x^j \in \langle 1, x, \dots, x^{n-1} \rangle$ para todo $j \in \mathbb{N}$, segue que $B[x] \subset \langle 1, x, \dots, x^{n-1} \rangle$. Por outro lado, como $\langle 1, x, \dots, x^{n-1} \rangle \subset B[x]$, segue que $B[x] = \langle 1, x, \dots, x^{n-1} \rangle$, ou seja, $B[x]$ é um B -módulo gerado por $\{1, x, \dots, x^{n-1}\}$.

(b) $\Rightarrow$ (c) Basta tomarmos $R = B[x]$

(c) $\Rightarrow$ (a) Seja $R = \langle y_1, \dots, y_n \rangle$ um B -módulo finitamente gerado, tal que $B \subset R$ e $x \in R$. Como $x \in R$ e R é subanel de A temos que $xy_i \in R$ para todo i , e assim $xy_i = \sum_{j=1}^n b_{ij}y_j$,

com $b_{ij} \in B$ para $1 \leq i, j \leq n$. Assim, $xy_i - \sum_{j=1}^n b_{ij}y_j = 0$, para $i = 1, \dots, n$, é um sistema linear homogêneo nas variáveis $y_1, \dots, y_n$, ou seja, $\sum_{j=1}^n b_{ij}y_j(\delta_{ij}x - b_{ij})y_j = 0$, sendo $\delta_{ij} = 1$

se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$. Sejam, $C = (\delta_{ij}x - b_{ij})_{n \times n}$ e $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$. Sabendo que

$(adj C) \cdot C = det(C) \cdot I$, onde $adj C$ é a matriz adjunta de C e I é a matriz identidade, segue que, $det(C) \cdot Y = 0$. Portanto $det(C)y_i = 0$ para todo i . Conseqüentemente, para todo $b \in R$, temos que $b = \sum_{i=1}^n r_i y_i$ com $r_i \in B$. Assim, $det(C)b = det(C) \sum_{i=1}^n r_i y_i = \sum_{i=1}^n r_i (det(C)y_i) = 0$, e em particular para $b = 1 \in R$, temos que $det(C) = 0$. Assim, $det(C) = 0$ é uma equação de dependência inteira de x , ou seja, x é inteiro sobre B . $\blacksquare$

Proposição 2.1.1 *Sejam A um anel, B um subanel de A e $x_1, \dots, x_n$ elementos de A tal que x_i é inteiro sobre $B[x_1, \dots, x_{i-1}]$, $i = 2, \dots, n$. Então, $B[x_1, \dots, x_n]$ é um B -módulo finitamente gerado.*

Demonstração: A demonstração será feita por indução sobre n . Para o caso $n = 1$ segue do Teorema 2.1.1. Suponhamos $n > 1$ e que a afirmação seja verdadeira para $n - 1$ elementos. Seja $B[x_1, \dots, x_n] = R[x_n]$, onde $R = B[x_1, \dots, x_{n-1}]$. Por hipótese de indução R é um B -módulo finitamente gerado, isto é, $R = \sum_{i=1}^s By_i$. Visto que x_n é inteiro sobre R temos que

$R[x_n]$ é um R -módulo finitamente gerado, isto é, $R[x_n] = \sum_{j=1}^t Rz_j$. Então,

$$B[x_1, \dots, x_n] = R[x_n] = \sum_{j=1}^t Rz_j = \sum_{j=1}^t \left(\sum_{i=1}^s By_i \right) z_j = \sum_{i,j} By_i z_j.$$

Assim, $B[x_1, \dots, x_n]$ é gerado por $\{y_i z_j\}$, com $1 \leq i \leq s$, $1 \leq j \leq t$. Portanto, $B[x_1, \dots, x_n]$ é um B -módulo finitamente gerado. $\blacksquare$

Corolário 2.1.1 *Sejam A um anel, B um subanel de A , x e y elementos de A inteiros sobre B . Então $x + y$, $x - y$ e xy são inteiros sobre B .*

Demonstração: Pela Proposição 2.1.1 temos que $B[x, y]$ é um B -módulo finitamente gerado. Como $x + y$, $x - y$ e xy pertencem a $B[x, y]$ pela parte (c) do Teorema 2.1.1, segue que, $x + y$, $x - y$ e xy são inteiros sobre B . $\blacksquare$

Sejam A um anel e B um subanel de A . Denotando por A' o conjunto dos elementos de A que são inteiros sobre B , segue diretamente dos resultados anteriores que A' é um subanel de A que contém B .

Definição 2.1.1 *Sejam A um anel e B um subanel de A . O anel A' é chamado **fecho inteiro** de B em A e quando A for um domínio, chamamos de **fecho inteiro** de A , ao fecho inteiro de A em seu corpo de frações $\mathbb{K}$. Dizemos que A é inteiro sobre B , se todo elemento de A é inteiro sobre B .*

Exemplo 2.1.2 *Temos que o anel de Gauss $\mathbb{Z}[i]$ é inteiro sobre o anel $\mathbb{Z}$, pois todo elemento $a + bi$ de $\mathbb{Z}[i]$ é raiz do polinômio $X^2 - 2aX + (a^2 + b^2) \in \mathbb{Z}[X]$, ou seja, todo elemento de $\mathbb{Z}[i]$ é inteiro sobre $\mathbb{Z}$.* $\blacksquare$

Proposição 2.1.2 *Sejam A um anel, B um subanel de A , e C um subanel de B . Então, A é inteiro sobre B e B é inteiro sobre C se, e somente se, A é inteiro sobre C .*

Demonstração: Seja $x \in A$. Então x é inteiro sobre B , ou seja, existem $b_0, \dots, b_{n-1} \in B$ tal que $x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$. Tomando $D = C[b_0, \dots, b_{n-1}]$, segue que x é inteiro sobre D . Como por hipótese B é inteiro sobre C , temos que os b_i são inteiros sobre C . Daí pela Proposição 2.1.1 temos que $D[x] = C[b_0, \dots, b_{n-1}, x]$ é um C -módulo finitamente gerado, e pela parte (c) do Teorema 2.1.1, segue que x é inteiro sobre C . Portanto, A é inteiro sobre C . Agora, suponhamos, que A é inteiro sobre C e seja $x \in A$. Então existem $c_0, c_1, \dots, c_{n-1} \in C$ tal que $x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0 = 0$. Como $C \subset B$, segue que x é inteiro sobre B , ou seja, A é inteiro sobre B . Se $x \in B$ como $B \subset A$, segue que x é inteiro sobre C , ou seja, B é inteiro sobre C . $\blacksquare$

Proposição 2.1.3 *Sejam A um domínio e B um subanel de A tal que A é inteiro sobre B . Então, A é um corpo se, e somente se, B é um corpo.*

Demonstração: Suponhamos que B é um corpo e seja $a \in A$; $a \neq 0$. Como a é inteiro sobre B , pelo Teorema 2.1.1, temos que $B[a]$ é um espaço vetorial de dimensão finita sobre B . Seja a B -transformação linear $\varphi : B[a] \rightarrow B[a]$, definida por $\varphi(b) = ba$, $\forall b \in B[a]$. Da hipótese de B ser um corpo, segue que $B[a]$ é um domínio, e então a B -transformação é injetiva e sobrejetora. Logo, existe $a' \in B[a]$, tal que $\varphi(a') = aa' = 1$. Portanto, a é invertível em A , ou seja, A é corpo. Por outro lado, seja $b \in B - (0)$. Como $B \subset A$, temos que b tem um inverso $b^{-1} \in A$. Como A é inteiro sobre B , então $b^{-n} + a_{n-1}b^{-n+1} + \dots + a_1b^{-1} + a_0 = 0$, com $a_i \in B$. Multiplicando essa equação por b^{n-1} temos que $b^{-1} + a_{n-1} + a_{n-2}b + \dots + a_1b^{n-2} + a_0b^{n-1} = 0$, e daí $b^{-1} = -(a_{n-1} + a_{n-2}b + \dots + a_1b^{n-2} + a_0b^{n-1}) \in B$. Portanto, B é corpo. $\blacksquare$

Definição 2.1.2 *Um anel A é chamado integralmente fechado quando A é um domínio e é seu próprio fecho inteiro. Em outras palavras, um anel A é integralmente fechado se todo elemento do seu corpo de frações que é inteiro sobre A está em A .*

Exemplo 2.1.3 *Seja A um domínio e seja $\mathbb{K}$ seu corpo de frações. Então o fecho inteiro A' de A , isto é, o fecho inteiro de A em $\mathbb{K}$ é integralmente fechado. Isso segue do fato de que o fecho inteiro de A' é inteiro sobre A' , portanto sobre A .* $\blacksquare$

Exemplo 2.1.4 *Todo anel fatorial é integralmente fechado. Em particular, todo anel principal é integralmente fechado. De fato, sejam A um anel fatorial e $x = \frac{a}{b}$ um elemento do*

corpo de frações de A inteiro sobre A , com $a, b \in A$ e $\text{mdc}\{a, b\} = 1$. Sendo x um elemento inteiro sobre A , temos que $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$, com $a_i \in A, i = 1, \dots, n-1$. Multiplicando esta equação por b^n , obtemos $a^n + a_{n-1}a^{n-1}b + \dots + a_1ab^{n-1} + a_0b^n = 0$. Deste modo temos, $a^n = b(-a_{n-1}a^{n-1} - \dots - a_1ab^{n-2} - a_0b^{n-1})$, e portanto, b divide a^n . Como $\text{mdc}\{a, b\} = 1$, segue que $a = bk$, com $k \in A$ e $ax_0 + by_0 = 1$ para algum $x_0, y_0 \in A$. Assim, $b(kx_0 + y_0) = 1$, ou seja, b é invertível em A . Logo $x \in A$. $\blacksquare$

Exemplo 2.1.5 O anel $\mathbb{Z}$ é integralmente fechado uma vez que $\mathbb{Z}$ é principal. $\blacksquare$

2.2 Elementos algébricos sobre um corpo e extensões algébricas

Sejam A um anel e K um subcorpo de A , ou seja, K é um subanel de A que tem estrutura de corpo. Dizemos que um elemento x de A é **algébrico** sobre K , se x é raiz de um polinômio não nulo, com coeficientes em K . Se todo elemento de A for algébrico sobre K , dizemos que A é algébrico sobre K . Um elemento de A que não é algébrico sobre K é dito transcendente sobre K .

Exemplo 2.2.1 O elemento $x = \sqrt{3} + \sqrt{-5}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio, $X^4 + 4X^2 + 64 \in \mathbb{Q}[X]$. $\blacksquare$

Segundo a definição, sendo x um elemento algébrico sobre um corpo K , x satisfaz uma equação do tipo, $a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$, com $a_i \in K, a_n \neq 0$. Multiplicando essa equação por a_n^{-1} , obtemos uma equação de dependência inteira, $x^n + a_n^{-1}a_{n-1}x^{n-1} + \dots + a_n^{-1}a_1x + a_n^{-1}a_0 = 0$, e portanto, sobre um corpo, o conceito de elemento algébrico coincide com o de elemento inteiro. Uma extensão L de K é dita algébrica se todo elemento de L é algébrico sobre K .

Dados $K \subset L$ corpos e α um elemento de L , o conjunto de todas as expressões polinomiais em α com coeficientes em K será denotado por $K[\alpha]$. A dimensão de L como espaço vetorial sobre K é chamada **grau** de L sobre K e denotado por $[L : K]$. Se $[L : K]$ é finito, então L é uma **extensão algébrica de grau finito** de K , e como sobre um corpo elemento algébrico

significa inteiro, podemos usar os resultados obtidos anteriormente sobre elementos inteiros para elementos algébricos. Assim, para $K \subset A$ e $x \in A$ um anel, x é algébrico sobre K se, e somente se, $[K[x] : K]$ é finito.

Um resultado muito útil de extensões algébricas é o de multiplicatividade de graus, ou seja, sendo K um corpo, L uma extensão algébrica de K e F uma extensão algébrica de L , tem-se que F é uma extensão algébrica de K e $[F : K] = [F : L] \cdot [L : K]$. Para vermos isto, basta considerarmos o conjunto, $S = \{v_i u_j\}$ onde $\{v_1, \dots, v_r\}$ é base de F sobre L e $\{u_1, \dots, u_s\}$ é base de L sobre K e verificar que, além de ser uma base da extensão L sobre K , sua cardinalidade é $[F : L] \cdot [L : K]$.

Sejam A um anel, K um subcorpo de A e a um elemento de A . Consideremos o seguinte homomorfismo de anéis, $\sigma_a : K[X] \rightarrow A$ definido por $\sigma_a(u) = u$, $\forall u \in K$, $\sigma_a(X) = a$ e estendido por linearidade. Assim, $\ker \sigma_a = \{f(X) \in K[X]; f(a) = 0\}$ e $\text{Im} \sigma_a = \{\sigma_a(f(X)); f(X) \in K[X]\} = \{f(a); f(X) \in K[X]\} = K[a]$. Através deste homomorfismo podemos redefinir elemento algébrico sobre K da seguinte forma: a é algébrico sobre K se $\ker \sigma_a \neq \{0\}$. Quando a é transcendente sobre K temos $K[a] \simeq K[X]$. Como $K[X]$ é um anel principal, então $\ker \sigma_a$ é um ideal principal, gerado por um polinômio $f(X) \in K[X]$, ou seja, $\ker \sigma_a = \langle f(X) \rangle$. Sendo a transcendente então $f(X)$ é o polinômio nulo, e se a é algébrico, então $f(X)$ é um polinômio não nulo e podemos supor neste caso, $f(X)$ mônico, pois K é corpo. Sob tais condições $f(X)$ é único e do fato de ser gerador do $\ker \sigma_a$, $f(X)$ tem grau mínimo dentre os polinômios que se anulam em a , sendo chamado de **polinômio minimal** de a sobre K e denotado por $\text{irr}(a, K)$ e seu grau é $\partial \text{irr}(a, K) = [K(a) : K]$.

Definição 2.2.1 *Sejam K um corpo e $f(X) \in K[X]$ um polinômio não constante. Dizemos que L é o corpo de raízes de $f(X)$ sobre K se, L é o menor corpo tal que $K \subset L$ e $f(X)$ se fatora completamente em L .*

Exemplo 2.2.2 *O corpo $L = \mathbb{Q}(\sqrt[3]{2}, \xi)$ é o corpo de raízes do polinômio $X^3 - 2 \in \mathbb{Q}[X]$ onde $\xi = e^{2\pi i/3}$.* ▀

Um corpo K é chamado **algebricamente fechado** se todo polinômio não constante $P(X) \in K[X]$ pode ser expresso como um produto de fatores lineares, todos pertencentes à $K[X]$. Como exemplo de um corpo algebricamente fechado temos $\mathbb{C}$, o corpo dos números

complexos. Dados dois corpos $\mathbb{L}$ e $\mathbb{L}'$ ambos contendo um corpo $\mathbb{K}$. Todo isomorfismo $\varphi : \mathbb{L} \rightarrow \mathbb{L}'$ tal que $\varphi(a) = a, \forall a \in \mathbb{K}$, é chamado um $\mathbb{K}$ -isomorfismo de $\mathbb{L}$ em $\mathbb{L}'$, e quando existir tal isomorfismo dizemos que $\mathbb{L}$ e $\mathbb{L}'$ são $\mathbb{K}$ -isomorfos, ou que eles são *conjugados* sobre $\mathbb{K}$. Dadas duas extensões $\mathbb{L}$ e $\mathbb{L}'$ de $\mathbb{K}$, dizemos que dois elementos $x \in \mathbb{L}$ e $x' \in \mathbb{L}'$ são conjugados sobre $\mathbb{K}$ se existe um $\mathbb{K}$ -isomorfismo $\varphi : \mathbb{K}(x) \rightarrow \mathbb{K}(x')$ tal que $\varphi(x) = x'$. A existência de um isomorfismo φ nos garante que x e x' são ambos transcendentess sobre $\mathbb{K}$ ou são ambos algébricos sobre $\mathbb{K}$ com o mesmo polinômio minimal.

Teorema 2.2.1 [3] *Sejam $\mathbb{K}$ um corpo, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau n e $\mathbb{F}$ um corpo algebricamente fechado contendo $\mathbb{K}$. Então existem n $\mathbb{K}$ -isomorfismos de $\mathbb{L}$ em $\mathbb{F}$.*

Temos que toda extensão de grau finito é uma extensão algébrica e toda extensão finita dos racionais, recebe o nome de **corpo de números**. Chamamos de **fecho algébrico** de $\mathbb{Q}$, o conjunto $\overline{\mathbb{Q}}$ de todos os números complexos algébricos sobre $\mathbb{Q}$. Como o corpo dos números complexos é algebricamente fechado, temos que o fecho algébrico dos racionais é um corpo algebricamente fechado. Uma extensão de corpos de grau 2 sobre o corpo $\mathbb{Q}$ é chamado de **corpo quadrático**.

Dado um corpo de números $\mathbb{K}$, vimos pelo Corolário 2.1.1 que o conjunto formado pelos elementos inteiros de $\mathbb{K}$ formam um anel, o qual denotaremos por $\mathcal{O}_{\mathbb{K}}$ e chamaremos de **anel dos inteiros de $\mathbb{K}$** .

Proposição 2.2.1 *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrados.*

Demonstração: Seja $\mathbb{K} = \mathbb{Q}(x)$ uma extensão quadrática de $\mathbb{Q}$. Seja $F(X) = X^2 + bX + c$, $b, c \in \mathbb{Q}$ o polinômio minimal de $x \in \mathbb{K}$. Resolvendo a equação quadrática $x^2 + bx + c = 0$ temos $2x = -b \pm \sqrt{b^2 - 4c}$. Assim, $\mathbb{K} = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{b^2 - 4c})$. Como $b^2 - 4c$ é um número racional, temos que $b^2 - 4c = \frac{r}{s} = \frac{rs}{s^2} \in \mathbb{Q}$, com $r, s \in \mathbb{Z}$. Assim, $\mathbb{Q}(x) = \mathbb{Q}\left(\sqrt{\frac{rs}{s^2}}\right) = \mathbb{Q}(\sqrt{rs})$.

Suponhamos que $rs = k^2d$, $k, d \in \mathbb{Z}$, com d livre de quadrados. Logo, $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{rs}) = \mathbb{Q}(\sqrt{k^2d}) = \mathbb{Q}(\sqrt{d})$. ▀

Se $d > 0$, $\mathbb{Q}(\sqrt{d})$ é chamado **corpo quadrático real** e se $d < 0$, $\mathbb{Q}(\sqrt{d})$ é chamado **corpo quadrático imaginário**. O elemento $\sqrt{d}$ é raiz do polinômio $X^2 - d$, e tem-se $-\sqrt{d}$

como seu conjugado em $\mathbb{K}$. Então existe um automorfismo σ de $\mathbb{K}$ que leva $\sqrt{d}$ em $-\sqrt{d}$, ou seja, $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$, com $a, b \in \mathbb{Q}$.

Seja $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de um corpo de números $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados. Seja $x \in \mathcal{O}_{\mathbb{K}}$. Então existem $a_0, \dots, a_{n-1} \in \mathbb{Z}$, tal que $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$. Assim, $\sigma(x^n) + a_{n-1}\sigma(x^{n-1}) + \dots + a_1\sigma(x) + a_0 = 0$, ou seja, $\sigma(x) \in \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}}$ é um anel, segue que $x + \sigma(x)$ e $x\sigma(x)$ pertencem a $\mathcal{O}_{\mathbb{K}}$. Tomando $x = a + b\sqrt{d} \in \mathbb{K}$, temos

$$x + \sigma(x) = a + b\sqrt{d} + a - b\sqrt{d} = 2a \in \mathbb{Q} \text{ e } x \cdot \sigma(x) = (a + b\sqrt{d}) \cdot (a - b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}.$$

Como $\mathbb{Z}$ é um anel principal e portanto integralmente fechado, temos que $2a \in \mathbb{Z}$ e $a^2 - db^2 \in \mathbb{Z}$. Deste modo, como $x = a + b\sqrt{d}$ é inteiro sobre $\mathbb{Z}$, temos que x é raiz do polinômio $X^2 - 2aX + a^2 - db^2 = 0$.

Teorema 2.2.2 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados, ou seja, $d \not\equiv 0 \pmod{4}$.*

(a) *Se $d \equiv 2$ ou $d \equiv 3 \pmod{4}$, então o anel $\mathcal{O}_{\mathbb{K}}$ dos inteiros de $\mathbb{K}$ é formado pelos elementos da forma $a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$.*

(b) *Se $d \equiv 1 \pmod{4}$, então o anel $\mathcal{O}_{\mathbb{K}}$ dos inteiros de $\mathbb{K}$ é formado pelos elementos da forma $\frac{1}{2}(u + v\sqrt{d})$, com $u, v \in \mathbb{Z}$, u e v de mesma paridade.*

Demonstração: Seja $x = a + b\sqrt{d}$, com $a, b \in \mathbb{Q}$, um elemento inteiro sobre $\mathbb{Z}$, isto é, $x \in \mathcal{O}_{\mathbb{K}}$. Se $b = 0$, então o polinômio minimal de x sobre $\mathbb{Q}$ é dado por $m(X) = X - a$, e como x é inteiro sobre $\mathbb{Z}$, $a \in \mathbb{Z}$. Se $b \neq 0$, o polinômio minimal de x sobre $\mathbb{Q}$, tem grau 2 e é dado por $m(X) = X^2 - 2aX + a^2 - db^2$, e então $2a, a^2 - db^2 \in \mathbb{Z}$. Como d é um inteiro livre de quadrados, $2b \in \mathbb{Z}$, pois se $2b$ não fosse inteiro, seu denominador teria um fator primo p , cujo quadrado p^2 não se cancelaria com algum fator de d , pois este não possui fatores quadrados, e assim, $d(2b)^2$ não seria inteiro. Logo, $2b \in \mathbb{Z}$. Assim, podemos escrever:

$$a = u/2, \quad b = v/2 \text{ com } u, v \in \mathbb{Z}. \quad (2.2.1)$$

Daí, podemos concluir que

$$(2a)^2 - d(2b)^2 \in 4\mathbb{Z}. \quad (2.2.2)$$

Substituindo a por $u/2$ e b por $v/2$, com $u, v \in \mathbb{Z}$ temos que $u^2 - dv^2 \in 4\mathbb{Z}$.

(I) Se $b \in \mathbb{Z}$, então por (2.2.1), temos que v é par. Logo, u é par e portanto, $a \in \mathbb{Z}$.

(II) Se $b \notin \mathbb{Z}$, então v é ímpar e $v^2 \equiv 1 \pmod{4}$. As possibilidades $\pmod{4}$ para u^2 são 0 ou 1. Mas, d é inteiro livre de quadrados, logo, não é múltiplo de 4. Assim, necessariamente $u^2 \equiv 1 \pmod{4}$ e $d \equiv 1 \pmod{4}$. Portanto, u é ímpar, o que implica que $a \notin \mathbb{Z}$.

(a) Se $d \equiv 2$ ou $3 \pmod{4}$, temos que u e v são pares, pois se v fosse ímpar teríamos $v^2 \equiv 1 \pmod{4}$. Assim, como $u^2 - dv^2 \in 4\mathbb{Z}$, temos que $u^2 \equiv dv^2 \equiv d \pmod{4}$, ou seja, $d \equiv 0 \pmod{4}$ ou $d \equiv 1 \pmod{4}$, o que é um absurdo. Portanto, concluímos que v é par, isto é, $v^2 \equiv 0 \pmod{4}$ e assim, $u^2 \equiv dv^2 \equiv 0 \pmod{4}$ o que implica que u é par. Logo, se $x = a + b\sqrt{d} \in \mathcal{O}_K$ temos que $x \in \mathbb{Z}[\sqrt{d}]$ e assim, $\mathcal{O}_K \subset \mathbb{Z}[\sqrt{d}]$. Por outro lado, tomando $x \in \mathbb{Z}[\sqrt{d}]$, temos que x é raiz do polinômio $X^2 - 2aX + a^2 - db^2 \in \mathbb{Z}[X]$. Logo, $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$. Portanto, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$

(b) Se $d \equiv 1 \pmod{4}$, então $u^2 - v^2 \equiv 0 \pmod{4}$, ou seja, u e v têm a mesma paridade, isto é, são ambos pares ou ímpares. Se u e v são pares então $a, b \in \mathbb{Z}$. Logo, $x = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Se u e v são ímpares, então $x = a + b\sqrt{d} = u/2 + v/2\sqrt{d} = (u - v)/2 + v \left((1 + \sqrt{d})/2 \right) \in \mathbb{Z} \left[\frac{(1 + \sqrt{d})}{2} \right]$. Portanto, $x \in \mathbb{Z} \left[\frac{(1 + \sqrt{d})}{2} \right]$. Logo, $\mathcal{O}_K \subset \mathbb{Z} \left[\frac{(1 + \sqrt{d})}{2} \right]$. Por outro lado, se $x = a + b \left(\frac{1 + \sqrt{d}}{2} \right) \in \mathbb{Z} \left[\frac{(1 + \sqrt{d})}{2} \right]$, com $a, b \in \mathbb{Z}$, temos que $2a + b \in \mathbb{Z}$ e $(a + b/2)^2 - d(b/2)^2 = a^2 + ab + (1 - d)b^2/4 \in \mathbb{Z}$, pois $d \equiv 1 \pmod{4}$. Logo, $\mathbb{Z} \left[\frac{(1 + \sqrt{d})}{2} \right] \subset \mathcal{O}_K$, pois os coeficientes do polinômio minimal de x , $m(X) = X^2 - (2a + b)X + a^2 + ab + (1 - d)b^2/4$ estão em $\mathbb{Z}$. Portanto, $\mathbb{Z} \left[\frac{(1 + \sqrt{d})}{2} \right] = \mathcal{O}_K$. ■

Exemplo 2.2.3 Seja $K = \mathbb{Q}(\sqrt{-1})$ um corpo quadrático. Seu anel dos inteiros, também chamado, anel de Gauss, é dado por $\mathcal{O}_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, onde $i = \sqrt{-1}$, pois $d = -1 \equiv 3 \pmod{4}$. ■

Segue do Teorema 2.2.2 que se $d \equiv 2$ ou $d \equiv 3 \pmod{4}$, temos que $\{1, \sqrt{d}\}$ é uma base de $\mathcal{O}_K$ como um $\mathbb{Z}$ -módulo e se $d \equiv 1 \pmod{4}$, temos que $\{1, \frac{1}{2}(1 + \sqrt{d})\}$ é uma base de $\mathcal{O}_K$ como um $\mathbb{Z}$ -módulo.

2.3 Norma e traço em uma extensão

Sejam A um anel e B um subanel de A , tal que A é um B -módulo livre de posto finito n . Para todo $x \in A$, temos que $m_x : A \rightarrow A$ definido por $y \mapsto xy$, é um endomorfismo do B -módulo A .

Definição 2.3.1 Chamamos de *traço*, respectivamente *norma* e *polinômio característico* de $x \in A$, relativo a A e B , o *traço*, respectivamente, *determinante* e *polinômio característico* do endomorfismo m_x . O polinômio característico é um polinômio mônico com coeficientes em B .

Denotamos o traço e a norma de x respectivamente por $Tr_{A/B}(x)$ e $\mathcal{N}_{A/B}(x)$, e quando não houver perigo de confusão denotaremos por $Tr(x)$ e $\mathcal{N}(x)$.

Para x e $x' \in A$ e $b \in B$, temos que $m_x + m_{x'} = m_{x+x'}$ e $m_x \circ m_{x'} = m_{xx'}$ e $m_{bx} = bm_x$, e além disso, a matriz de m_b com respeito a alguma base de B sobre A é a matriz diagonal cuja as entradas são b .

Proposição 2.3.1 Sejam K um corpo, L uma extensão algébrica de K de grau n , x um elemento de L e $x_1, \dots, x_n$ as raízes do polinômio minimal de x sobre K . Então $Tr_{L/K}(x) = \sum_{i=1}^n x_i$ e $\mathcal{N}_{L/K}(x) = \prod_{i=1}^n x_i$. O polinômio característico de x , relativo a L e K é dado por $(X - x_1) \dots (X - x_n)$.

Demonstração: Trataremos primeiramente do caso em que x é um elemento primitivo de L sobre K . Seja $F(X)$ o polinômio minimal de x sobre K . Então L é K -isomorfo a $K[X]/\langle F(X) \rangle$ e $\{1, x, \dots, x^{n-1}\}$ é uma base de L sobre K . Tomando $F(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$, com $a_i \in K$, a matriz do endomorfismo m_x com respeito a esta base é dado por

$$M = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 0 & -a_{n-1} \end{bmatrix}.$$

O determinante de $X I_L - m_x$ é o determinante da matriz

$$XI_n - M = \begin{bmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & X & a_{n-2} \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{bmatrix}.$$

Expandindo esse determinante como um polinômio em X , obtemos o polinômio característico de x , que é igual a $F(X)$ e temos que $Tr(x) = -a_{n-1}$ e $\mathcal{N}(x) = (-1)^n a_0$. Como x é primitivo, temos que $F(X) = (X - x_1) \cdots (X - x_n)$, e equiparando os coeficientes vemos que $Tr(x) = x_1 + \cdots + x_n$ e $\mathcal{N}(x) = x_1 \cdots x_n$. Consideremos agora o caso geral. Colocando $r = [\mathbb{L} : \mathbb{K}[x]]$, é suficiente mostrarmos que o polinômio característico $P(X)$ de x , com respeito a $\mathbb{L}$ e $\mathbb{K}$, é igual a r -ésima potência do polinômio minimal de x sobre $\mathbb{K}$. Seja $\{y_i\}_{i=1, \dots, q}$ uma base de $\mathbb{K}[x]$ sobre $\mathbb{K}$ e seja $\{z_j\}_{j=1, \dots, r}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}[x]$. Então $\{y_i z_j\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $n = qr$. Se $M = (a_{ih})$ é a matriz de multiplicação por x em $\mathbb{K}[x]$ com relação a base $\{y_i\}$, temos que $xy_i = \sum_h a_{ih} y_h$. Então temos, $x(y_i z_j) = \left(\sum_h a_{ih} y_h \right) z_j = \sum_h a_{ih} (y_h z_j)$. Ordenamos a base $\{y_i z_j\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, de modo que a matriz M_1 da multiplicação por x em $\mathbb{L}$ com respeito a esta base tenha a seguinte forma:

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

isto é, M aparece r -vezes na diagonal como blocos na matriz M_1 . Daí, a matriz $XI_n - M_1$ consiste de r blocos diagonais, cada uma tem a forma $XI_q - M$. Conseqüentemente, $\det(XI_n - M_1) = \det(XI_q - M)^r$. Por outro lado, $P(X) = \det(XI_q - M)$ é o polinômio característico de x sobre $\mathbb{K}$, de acordo com a primeira parte da demonstração. $\blacksquare$

Proposição 2.3.2 *Sejam A um domínio, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau finito, e x um elemento de $\mathbb{L}$ inteiro sobre A e assumindo $\mathbb{K}$ de característica zero.*

Então os coeficientes do polinômio característico $P(X)$ de x relativo a $\mathbb{L}$ e $\mathbb{K}$, e em particular, $Tr_{\mathbb{L}/\mathbb{K}}(x)$ e $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(x)$, são inteiros sobre A .

Demonstração: Da Proposição 2.3.1, temos que $P(X) = (X - x_1) \dots (X - x_n)$. Como os coeficientes de $P(X)$ a menos de sinal, são somas de produtos dos x'_i s, é suficiente mostrarmos que cada x_i é inteiro sobre A . Mas cada x_i é um conjugado de x sobre $\mathbb{K}$, ou seja, existe um $\mathbb{K}$ -isomorfismo $\sigma_i : \mathbb{K}[x] \rightarrow \mathbb{K}[x_i]$, tal que $\sigma_i(x) = x_i$. Assim, aplicando σ_i na equação de dependência inteira de x sobre A , obtemos uma equação de dependência inteira de x_i sobre A . Assim, cada x_i é inteiro sobre A , portanto $Tr_{\mathbb{L}/\mathbb{K}}(x)$ e $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(x)$, são inteiros sobre A . ▀

Corolário 2.3.1 Com as condições da Proposição 2.3.2, se A é um anel integralmente fechado, então os coeficientes do polinômio característico de x , e em particular, $Tr_{\mathbb{L}/\mathbb{K}}(x)$ e $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(x)$ são elementos de A .

Demonstração: Por definição esses coeficientes são elementos de $\mathbb{K}$. Pela Proposição 2.3.2 são inteiros sobre A . Logo, são elementos de A , pois A é integralmente. ▀

Sejam $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ corpos de números, $x, y \in \mathbb{M}$ e $a \in \mathbb{K}$. Então valem as seguintes propriedades:

$$1. \mathcal{N}_{\mathbb{M}/\mathbb{K}}(xy) = \mathcal{N}_{\mathbb{M}/\mathbb{K}}(x)\mathcal{N}_{\mathbb{M}/\mathbb{K}}(y),$$

$$2. Tr_{\mathbb{M}/\mathbb{K}}(x + y) = Tr_{\mathbb{M}/\mathbb{K}}(x) + Tr_{\mathbb{M}/\mathbb{K}}(y),$$

$$3. Tr_{\mathbb{M}/\mathbb{K}}(ax) = aTr_{\mathbb{M}/\mathbb{K}}(x),$$

$$4. Tr_{\mathbb{M}/\mathbb{K}}(a) = [\mathbb{M} : \mathbb{K}]a,$$

$$5. \mathcal{N}_{\mathbb{M}/\mathbb{K}}(a) = a^{[\mathbb{M}:\mathbb{K}]},$$

$$6. \mathcal{N}_{\mathbb{M}/\mathbb{K}}(x) = \mathcal{N}_{\mathbb{L}/\mathbb{K}}(\mathcal{N}_{\mathbb{M}/\mathbb{L}}(x)),$$

$$7. Tr_{\mathbb{M}/\mathbb{K}}(x) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(x)).$$

2.4 Discriminante

Esta seção tem como objetivo introduzir o conceito de discriminante via o determinante de uma matriz.

Definição 2.4.1 Sejam A um anel e B um subanel de A , tal que A é um B -módulo livre de posto finito n . Dado $(x_1, \dots, x_n) \in A^n$ chamamos o discriminante do conjunto $(x_1, \dots, x_n)$ o elemento de B definido pela relação $D(x_1, \dots, x_n) = \det(\text{Tr}_{A/B}(x_i x_j))$.

Exemplo 2.4.1 Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\{1, \sqrt{7}\} \subset \mathbb{K}$. Então,

$$D(1, \sqrt{7}) = \begin{vmatrix} \text{Tr}(1) & \text{Tr}(\sqrt{7}) \\ \text{Tr}(\sqrt{7}) & \text{Tr}(\sqrt{7})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 14 \end{vmatrix} = 28. \quad \blacksquare$$

Proposição 2.4.1 Se $(y_1, \dots, y_n) \in A^n$ é outro conjunto de elementos de A , tal que $y_i = \sum_{j=1}^n a_{ij} x_j$ com $a_{ij} \in B$, então $D(y_1, \dots, y_n) = (\det(a_{ij}))^2 D(x_1, \dots, x_n)$.

Demonstração: Tomando $y_p = \sum_i a_{pi} x_i$ e $y_q = \sum_j a_{qj} x_j$, segue que $y_p y_q = \sum_{i,j} a_{pi} a_{qj} x_i x_j$, e

assim $\text{Tr}(y_p y_q) = \text{Tr}\left(\sum_{i,j} a_{pi} a_{qj} x_i x_j\right) = \sum_{i,j} a_{pi} a_{qj} \text{Tr}(x_i x_j)$. Isto nos dá a equação matricial $(\text{Tr}(y_p y_q)) = (a_{pi})(\text{Tr}(x_i x_j))(a_{qj})^t$, e tomando agora o determinante segue o resultado. $\blacksquare$

Exemplo 2.4.2 Pelo Exemplo 2.4.1 vimos que o discriminante da base $\{1, \sqrt{7}\}$ do corpo de números $\mathbb{K} = \mathbb{Q}(\sqrt{7})$ é igual a 28. Agora considerando uma outra base para o corpo $\mathbb{K}$, por exemplo $\{2 - \sqrt{7}, 5 + \sqrt{7}\}$, segue pela Proposição 2.4.1 que

$$D(2 - \sqrt{7}, 5 + \sqrt{7}) = \left(\det \begin{pmatrix} 2 & -1 \\ 5 & 2 \end{pmatrix} \right)^2 D(1, \sqrt{7}) = 9^2 \cdot 28. \quad \blacksquare$$

A Proposição 2.4.1 implica que o discriminante das bases de A sobre B são associados, isto é, a matriz (a_{ij}) que expressa uma base em termos da outra tem uma matriz inversa com entradas em B . Portanto, ambos $\det(a_{ij})$ e $\det(a_{ij})^{-1}$ são invertíveis em B . Com isso temos a seguinte definição.

Definição 2.4.2 Sejam A um anel e B um subanel de A , tal que A é um B -módulo livre de posto finito n . Chamamos de **discriminante de A sobre B** , o ideal principal de B gerado pelo discriminante das bases de A sobre B , e denotamos por $\mathfrak{D}_{A/B}$.

Proposição 2.4.2 Suponhamos que $\mathfrak{D}_{A/B}$ contém um elemento que não é um divisor de zero. Então, $(x_1, \dots, x_n) \subset A^n$ é uma base de A sobre B se, e somente se, $D(x_1, \dots, x_n)$ gera $\mathfrak{D}_{A/B}$.

Demonstração: Se $\{x_1, x_2, \dots, x_n\}$ é uma base de A sobre B , então pela Proposição 2.4.1, segue que $D(x_1, \dots, x_n)$ gera $\mathfrak{D}_{A/B}$. Reciprocamente, suponhamos que $d = D(x_1, \dots, x_n)$ gera $\mathfrak{D}_{A/B}$. Sejam $\{e_1, \dots, e_n\}$ uma base de $\mathfrak{D}_{A/B}$, $d' = D(e_1, \dots, e_n)$ e $x_i = \sum_{j=1}^n b_{ij}e_j$ com $b_{ij} \in B, i = 1, \dots, n$. Então, $d = \det(a_{ij})^2 d'$. Por hipótese, $Bd = \mathfrak{D}_{A/B} = Bd'$. Portanto, existe um elemento $a \in B$, tal que $d' = ad$. Então $d = \det(a_{ij})^2 ad$, e portanto, $d(1 - \det(a_{ij})^2 a) = 0$. Temos que d não é um divisor de zero, pois se fosse todo elemento de $Bd = \mathfrak{D}_{A/B}$ seria um divisor de zero. Portanto, $1 - \det(a_{ij})^2 a = 0$, daí $\det(a_{ij})$ é invertível. Assim, a matriz $M = [a_{ij}]$ é invertível. Então, $\{x_1, \dots, x_n\}$ é base de A sobre B . $\blacksquare$

Lema 2.4.1 (Dedekind) *Sejam G um grupo, $\mathbb{F}$ um corpo, e $\sigma_1, \dots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo $\mathbb{F}^*$. Então, os σ_i 's são linearmente independentes sobre o corpo $\mathbb{F}$.*

Demonstração: Suponhamos que os σ_i 's são linearmente dependentes. Assim existe uma relação não trivial $\sum_i u_i \sigma_i = 0$, com $u_i \in \mathbb{F}$, onde o número q dos u_i 's não nulos é mínimo. Agora renumerando os u_i 's, podemos supor que

$$u_1 \sigma_1(g) + \dots + u_q \sigma_q(g) = 0, \forall g \in G. \quad (2.4.3)$$

Temos que $q \geq 2$, pois os σ_i 's são não todos nulos. Dados g e h em G , temos que

$$u_1 \sigma_1(hg) + \dots + u_q \sigma_q(hg) = u_1 \sigma_1(h) \sigma_1(g) + \dots + u_q \sigma_q(h) \sigma_q(g) = 0. \quad (2.4.4)$$

Multiplicado (2.4.3) por $\sigma_1(h)$ e subtraindo (2.4.4) temos,

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_2(g) + \dots + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

Como isso vale para todo $g \in G$ e q foi escolhido como o menor possível, segue que $u_2(\sigma_1(h) - \sigma(h)) = 0$, ou seja, $\sigma_1(h) = \sigma(h)$ para todo $h \in G$, visto que $u_2 \neq 0$, o que contradiz a hipótese de que os homomorfismos são distintos. $\blacksquare$

Proposição 2.4.3 *Sejam $\mathbb{K}$ um corpo, $\mathbb{L}$ um extensão de $\mathbb{K}$ de grau finito n , e seja $\sigma_1, \dots, \sigma_n$ os n $\mathbb{K}$ -isomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{K}$. Então, se $\{x_1, \dots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, temos que $D(x_1, \dots, x_n) = \det(\sigma_i(x_j))^2 \neq 0$.*

Demonstração: Temos que $D(x_1, \dots, x_n) = \det(\text{Tr}(x_i x_j))$. Tomando o polinômio minimal de $x_i x_j$, o seu traço é a soma dos seus conjugados. Assim, $D(x_1, \dots, x_n) = \det(\text{Tr}(x_i x_j)) = \det\left(\sum_{k=1}^n \sigma_k(x_i x_j)\right) = \det\left(\sum_{k=1}^n \sigma_k(x_i) \sigma_k(x_j)\right) = \det(\sigma_k(x_i)) \det(\sigma_k(x_j)) = (\det(\sigma_k(x_i x_j)))^2$, uma vez que

$$\begin{bmatrix} \sigma_1(x_1) & \sigma_2(x_1) & \cdots & \sigma_n(x_1) \\ \sigma_1(x_2) & \sigma_2(x_2) & \cdots & \sigma_n(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(x_n) & \sigma_2(x_n) & \cdots & \sigma_n(x_n) \end{bmatrix} \begin{bmatrix} \sigma_1(x_1) & \sigma_1(x_2) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(x_1) & \sigma_n(x_2) & \cdots & \sigma_n(x_n) \end{bmatrix} = \sum_{k=1}^n \sigma_k(x_i x_j).$$

Para mostrar que $\det(\sigma_k(x_j)) \neq 0$, vamos supor por absurdo que $\det(\sigma_k(x_j)) = 0$. Então, existem $a_1, \dots, a_n \in F$, não todos nulos, tal que $\sum_{i=1}^n a_i \sigma_i(x_j) = 0$ para todo j . Dado $x \in L$, então $x = \sum_{i=1}^n b_i x_i$, com $b_i \in K$, e por linearidade concluímos que $\sum_{i=1}^n a_i \sigma_i(x) = 0$ o que contradiz o Lema de Dedekind. $\blacksquare$

Corolário 2.4.1 *Sejam A um anel integralmente fechado, L uma extensão finita de K de grau finito n e A' o fecho inteiro de A em L . Então a forma bilinear $\varphi : L \times L \rightarrow K$ definida por $\varphi(x, y) = \text{Tr}_{L/K}(x, y)$ é não degenerada, isto é, se $\text{Tr}_{L/K}(x, y) = 0$ para todo $y \in L$, então $x = 0$.*

Demonstração: Seja $\{x_1, \dots, x_n\}$ uma base de L sobre K . Seja $x \in L$. É suficiente mostrar que se $\text{Tr}(x_i x_j) = 0$, para todo $j = 1, \dots, n$, então $x = 0$. Temos que $x = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_n x_n$, com $\alpha_i \in K$, $i = 1, \dots, n$. Assim, se $\alpha_1 \text{Tr}(x_1 x_j) + \alpha_2 \text{Tr}(x_2 x_j) + \dots + \alpha_n \text{Tr}(x_n x_j) = \text{Tr}(x x_j) = 0$, para todo $j = 1, \dots, n$, então obtemos o seguinte sistema linear homogêneo

$$\begin{bmatrix} \text{Tr}(x_1 x_1) & \text{Tr}(x_1 x_2) & \cdots & \text{Tr}(x_1 x_n) \\ \text{Tr}(x_2 x_1) & \text{Tr}(x_2 x_2) & \cdots & \text{Tr}(x_2 x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Tr}(x_n x_1) & \text{Tr}(x_n x_2) & \cdots & \text{Tr}(x_n x_n) \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Da Proposição 2.4.3, temos que $\det(\text{Tr}(x_i x_j)) \neq 0$, e portanto o sistema possui solução única dada por $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$. Portanto, $x = 0$. $\blacksquare$

Observação 2.4.1 Segue do Corolário 2.4.1 que a aplicação $\mathbb{K}$ -linear $\psi : \mathbb{L} \rightarrow \text{Hom}_{\mathbb{L}}(\mathbb{L}, \mathbb{K})$ definida por $\psi(x) = \psi_x$, onde $\psi_x(y) = \text{Tr}(xy)$, para $x, y \in \mathbb{L}$, é injetiva. Temos que $\text{Ker}(\psi) = \{0\}$, ou seja, ψ é injetora, e como $\dim_{\mathbb{K}} \mathbb{L} = \dim_{\mathbb{K}} \mathbb{L}^*$, segue que ψ é sobrejetora, ou seja, ψ é bijetora. Assim, se $\{x_1, \dots, x_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então existe $\{\psi_{y_1}, \dots, \psi_{y_n}\}$ base dual de $\text{Hom}_{\mathbb{L}}(\mathbb{L}, \mathbb{K})$, tal que $\text{Tr}(xx_j) = \psi_{y_i}(x_j) = \delta_{ij}$. $\blacksquare$

Teorema 2.4.1 Sejam A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau finito n , e A' o fecho inteiro de A em $\mathbb{L}$. Suponha $\mathbb{K}$ com característica zero. Então A' é um A -submódulo de um A -módulo livre de posto n .

Demonstração: Seja $\{x_1, \dots, x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como cada x_i é algébrico sobre $\mathbb{K}$, temos que para todo i , existe uma equação da forma $a_n x_i^n + a_{n-1} x_i^{n-1} + \dots + a_0 = 0$, com $a_j \in A$, para todo j . Supondo que $a_n \neq 0$ e multiplicando esta equação por a_n^{n-1} , vemos que $a_n x_i$ é inteiro sobre A . De fato, $a_n^{n-1}(a_n x_i^n + a_{n-1} x_i^{n-1} + \dots + a_0) = 0 = (a_n x_i)^n + a_{n-1} x_i^{n-1} + \dots + a_n^{n-2}(a_n x_i) + a_n^{n-1} a_0$. Logo, $a_n x_i \in A'$, e então $a_n x_i = x'_i$, com $x'_i \in A'$. Portanto, $\{x'_1, \dots, x'_n\}$ forma uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em A' , uma vez que se $\alpha_1 x'_1 + \dots + \alpha_n x'_n = 0$ com $\alpha_i \in \mathbb{K}$, então $\alpha_1(a_n x_1) + \dots + \alpha_n(a_n x_n) = 0$, ou seja, $(\alpha_1 a_n)x_1 + \dots + (\alpha_n a_n)x_n = 0$. Como $\{x_1, \dots, x_n\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $\alpha_i a_i = 0$, para todo i , e como $a_n \neq 0$, segue que $\alpha_i = 0$, para todo i , o que prova que $\{x'_1, \dots, x'_n\}$ é linearmente independente, e como possui n elementos, segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pela Observação 2.4.1 existe uma base $\{y_1, \dots, y_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, tal que $\text{Tr}(x'_i y_j) = \delta_{ij}$. Tomando $z \in A'$, e como $\{y_1, \dots, y_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, escrevemos $z = \sum_{j=1}^n b_j y_j$ com $b_j \in \mathbb{K}$. Para todo i temos $x'_i z \in A'$, uma vez que $x'_i \in A$. Portanto, pelo Corolário 2.3.1, temos que $\text{Tr}(x'_i z) \in A$. Assim, como $\text{Tr}(x'_i z) = \text{Tr}\left(\sum_j b_j x'_i y_j\right) = \sum_j b_j \text{Tr}(x'_i y_j) = \sum_j b_j \delta_{ij} = b_i$, concluímos que $b_i \in A$, $\forall i$, o que implica que A' é um submódulo do A -módulo livre $\sum_{j=1}^n A y_j$. $\blacksquare$

Corolário 2.4.2 Com as hipóteses do Teorema 2.4.1, se A um anel principal, então A' é um A -módulo livre de posto n .

Demonstração: Pelo Teorema 1.1.3 temos que um submódulo de um A -módulo livre com A principal é livre com posto $\leq n$. Por outro lado, vimos no Teorema 2.4.1 que A' contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$, logo seu posto é n . $\blacksquare$

Definição 2.4.3 Seja $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o seu anel dos inteiros, temos que $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$ -módulo livre de posto $[\mathbb{K} : \mathbb{Q}]$, cuja base é chamada de **base integral**, e seu discriminante é chamado **discriminate absoluto**.

Proposição 2.4.4 Sejam $\mathbb{K}$ um corpo e $\mathbb{L} = \mathbb{K}[\alpha]$ uma extensão finita de $\mathbb{K}$ de grau n e $f(x)$ o polinômio minimal de α sobre $\mathbb{K}$. Então, $D(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} \mathcal{N}_{\mathbb{L}/\mathbb{K}}(f'(\alpha))$, onde $f'(\alpha)$ é a derivada de $f(\alpha)$.

Demonstração: Se $\alpha_1, \dots, \alpha_n$ são as raízes de $f(x)$ em alguma extensão de $\mathbb{K}$, então são os conjugados de α . Assim, pela Proposição 2.4.3 temos que $D(1, \alpha, \dots, \alpha^{n-1}) = \det(\sigma_i(\alpha_j))^2 = \det(\alpha_i^j)^2 = \left[\prod_{i>j} (\alpha_i - \alpha_j) \right]^2 = (-1)^{\frac{1}{2}n(n-1)} \prod_i \left(\prod_{i \neq j} (\alpha_i - \alpha_j) \right) = (-1)^{\frac{1}{2}n(n-1)} \prod_i f'(\alpha_i) = (-1)^{\frac{1}{2}n(n-1)} \mathcal{N}_{\mathbb{L}/\mathbb{K}}(f'(\alpha))$. Em particular, se $f(x) = x^n + ax + b$, temos que $D(1, \alpha, \dots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} (n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n)$. ■

Exemplo 2.4.3 Sejam $K = \mathbb{Q}(\alpha)$, com $\alpha = \sqrt[3]{2}$ e $f(X) = X^3 - 2 = \text{irr}(\alpha, \mathbb{Q})$. Então, $\Delta[1, \alpha, \alpha^2] = (-1)^3 \cdot \mathcal{N}_{K/\mathbb{Q}}(3\alpha^2) = -(3\alpha^2)^3 = -27 \cdot 4$. ■

2.5 Corpos ciclotômicos

Uma raiz α da unidade sobre $\mathbb{Q}$ é uma raiz do polinômio $X^n - 1$, e neste caso dizemos que α é uma raiz n -ésima da unidade. Um **corpo ciclotômico** é um corpo numérico gerado pelas raízes da unidade sobre $\mathbb{Q}$. Dado um número primo p , denotemos por ξ uma raiz p -ésima primitiva da unidade. Seja o corpo ciclotômico $\mathbb{Q}[\xi]$. O número ξ é uma raiz do polinômio $X^p - 1$, e desde que $\xi \neq 1$, ξ é também raiz do polinômio $(X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \dots + X + 1$, chamado de **polinômio ciclotômico**.

Teorema 2.5.1 (Critério de irreduzibilidade de Eisenstein) Sejam A um anel principal, p um elemento primo de A e $f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$, tal que p divide a_i , para $i = 1, \dots, n-1$, e p^2 não divide a_0 . Então, $f(X)$ é irreduzível sobre o corpo de frações $\mathbb{K}$ de A .

Demonstração: Suponhamos que $f(X)$ seja redutível, ou seja, $f(X) = g(X)h(X)$ com $g(X), h(X) \in \mathbb{K}[X]$ polinômios mônicos. Como toda raiz de $g(X)$ ou $h(X)$ é raiz de $f(X)$ e

que as raízes de $f(X)$ são inteiros sobre A , segue que as raízes de $g(X)$ e $h(X)$ são inteiros sobre A . Mas como A é principal, ou seja, é integralmente fechado, segue que $g(X) \in A[X]$ e $h(X) \in A[X]$. Agora, sejam $\overline{f(X)}$, $\overline{g(X)}$ e $\overline{h(X)}$ as imagens de $f(X)$, $g(X)$ e $h(X)$ em $\frac{A}{Ap}[X]$. Assim, $\overline{f(X)} = \overline{g(X)} \overline{h(X)}$. Como p divide a_i , para $i = 1, \dots, n-1$, segue que $\overline{f(X)} = X^n$, e desde que A/Ap é um domínio, segue que $X^n = X^q X^{n-q}$, uma vez que $g(X)$ e $h(X)$ são mônicos, e portanto, $\overline{g(X)} = X^q$ e $\overline{h(X)} = X^{n-q}$. Como $g(X)$ e $h(X)$ não são constantes, segue que p divide o termo constante de $g(X)$ e de $h(X)$, e isto contradiz a hipótese que p^2 não divide a_0 . Portanto, f é irredutível. $\blacksquare$

Teorema 2.5.2 *Se p um número primo, então o polinômio ciclotômico $X^{p-1} + X^{p-2} + \dots + X + 1$ é irredutível em $\mathbb{Q}[X]$.*

Demonstração: Fazendo $X = Y + 1$, temos que $X^{p-1} + X^{p-2} + \dots + X + 1 = \frac{X^p - 1}{X - 1} = \frac{(Y + 1)^p - 1}{Y} = Y^{p-1} + \sum_{j=p-1}^1 \binom{p}{j} Y^{j-1} = F_1(Y)$. Se $F_1(Y)$ for irredutível, então o polinômio

ciclotômico também será. Observando que p divide cada coeficiente binomial $\binom{p}{j}$ e que

p^2 não divide o termo constante $\binom{p}{1} = p$, concluímos pelo Critério de Eisenstein que $F_1(Y)$ é irredutível. $\blacksquare$

Segue do Teorema 2.5.2 que $[\mathbb{Q}[\xi] : \mathbb{Q}] = p - 1$ e que, $\{1, \xi, \dots, \xi^{p-2}\}$ é uma base de $\mathbb{Q}[\xi]$ sobre $\mathbb{Q}$. Nosso próximo objetivo é mostrarmos que $\mathbb{Z}[\xi]$ é o anel dos inteiros de $\mathbb{Q}[\xi]$.

Lema 2.5.1 *Sejam p um número primo e ξ uma raiz p -ésima primitiva da unidade em $\mathbb{C}$. Então*

- (i) $\text{Tr}(\xi^j) = -1$, $\forall j = 1, \dots, p-1$
- (ii) $\text{Tr}(1 - \xi^j) = p$, $\forall j = 1, \dots, p-1$
- (iii) $\mathcal{N}(\xi - 1) = (-1)^{p-1} p$ e $\mathcal{N}(1 - \xi) = p$
- (iv) $p = (1 - \xi)(1 - \xi^2) \dots (1 - \xi^{p-1})$

Demonstração: (i) O polinômio ciclotômico de ξ é dado por $f(X) = X^{p-1} + X^{p-2} + \dots + X + 1$. Portanto, como ξ^j são as raízes de $f(X)$, segue que $\text{Tr}(\xi^j) = -1$, para $j = 1, \dots, p-1$. Além disso, como $[\mathbb{Q}[\xi] : \mathbb{Q}] = p - 1$, segue que $\text{Tr}(1) = p - 1$. Para

(ii), temos que $Tr(1 - \xi^j) = Tr(1) - Tr(\xi^j) = p$, para $j = 1, \dots, p-1$. Para (iii) temos que $\xi - 1$ é raiz de $f(Y) = Y^{p-1} + \sum_{j=p-1}^1 \binom{p}{j} Y^{j-1}$, e portanto, $\mathcal{N}(\xi - 1) = (-1)^{p-1}p$ e $\mathcal{N}(1 - \xi) = \mathcal{N}((-1)(\xi - 1)) = (-1)^{p-1}\mathcal{N}(\xi - 1) = p$. Finalmente, para (iv) como $\mathcal{N}(1 - \xi)$ é o produto de seus conjugados, segue que $p = (1 - \xi)(1 - \xi^2) \dots (1 - \xi^{p-1})$.

Teorema 2.5.3 *Sejam p um número e ξ uma raiz p -ésima primitiva da unidade em $\mathbb{C}$. Então, o anel dos inteiros de $\mathbb{Q}[\xi]$ é $\mathbb{Z}[\xi]$ e $\{1, \xi, \dots, \xi^{p-2}\}$ é uma base do $\mathbb{Z}$ -módulo $\mathbb{Z}[\xi]$.*

Demonstração: Seja $\mathcal{O}_K$ o anel dos inteiros de $\mathbb{Q}[\xi]$. Assim, $\xi^j \in \mathcal{O}_K$, para $j = 1, \dots, p-1$, uma vez que são raízes do polinômio ciclotômico $f(X) = X^{p-1} + X^{p-2} + \dots + X + 1$. Agora, vamos mostrar que $\mathcal{O}_K(1 - \xi) \cap \mathbb{Z} = p\mathbb{Z}$. Pelo Lema 2.5.1, temos que $p \in \mathcal{O}_K(1 - \xi)$, e portanto, $p\mathbb{Z} \subset \mathcal{O}_K(1 - \xi) \cap \mathbb{Z}$. Como $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$, segue que se $p\mathbb{Z} \subsetneq \mathcal{O}_K(1 - \xi) \cap \mathbb{Z}$, e então $\mathcal{O}_K(1 - \xi) \cap \mathbb{Z} = \mathbb{Z}$, e portanto, $1 - \xi$ é invertível em $\mathcal{O}_K$. Assim, $1 - \xi^j$, para $j = 1, \dots, p-1$, são invertíveis em $\mathcal{O}_K$, e pelo Lema 2.5.1, segue que p é invertível em $\mathcal{O}_K \cap \mathbb{Z}$, o que é um absurdo. Assim, $p\mathbb{Z} = \mathcal{O}_K(1 - \xi) \cap \mathbb{Z}$. Agora, como $1 - \xi^j = (1 - \xi)(1 + \xi + \dots + \xi^{j-1})$ segue que cada conjugado $y_j(1 - \xi^j)$, para $j = 1, \dots, p-1$ e $y \in \mathcal{O}_K$ de $y(1 - \xi)$ é um múltiplo em $\mathcal{O}_K$ de $1 - \xi^j$ que também é um múltiplo de $1 - \xi$. Como o traço é a soma dos conjugados, segue que $Tr(y(1 - \xi)) \in \mathcal{O}_K(1 - \xi)$. Como $\mathbb{Z}$ é integralmente fechado, segue que $Tr(y(1 - \xi)) \in \mathbb{Z}$, e portanto, $Tr(y(1 - \xi)) \in p\mathbb{Z}$, para todo $y \in \mathcal{O}_K$. Finalmente, se $x = a_0 + a_1\xi + \dots + a_{p-2}\xi^{p-2}$, com $a_i \in \mathbb{Q}$ é um elemento de $\mathcal{O}_K$, temos que $x(1 - \xi) = a_0(1 - \xi) + a_1(\xi - \xi^2) + \dots + a_{p-2}(\xi^{p-2} - \xi^{p-1})$, e portanto, $Tr(x(1 - \xi)) = a_0Tr(1 - \xi) = a_0p \in p\mathbb{Z}$, ou seja, $a_0 \in \mathbb{Z}$. Como $(x - a_0)^{-1} = a_1 + a_2\xi + \dots + a_{p-2}\xi^{p-3} \in \mathcal{O}_K$, pois $\xi^{-1} = \xi^{p-1} \in \mathcal{O}_K$, o mesmo argumento mostra que $a_i \in \mathbb{Z}$ para todo i , ou seja, $\mathbb{Z}[\xi]$ é o anel dos inteiros de $\mathbb{Q}[\xi]$. ■

Corolário 2.5.1 *Sejam p um número primo, $r \geq 0$ e ξ uma raiz p^r -ésima primitiva da unidade. Então,*

- (i) *O polinômio minimal de ξ sobre $\mathbb{Q}$ é $X^{p^{r-1}} + X^{p^{r-1}(p-2)} + \dots + X^{p^{r-1}} + 1 = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}$.*
- (ii) $[\mathbb{Q}[\xi] : \mathbb{Q}] = p^{r-1}(p-1)$.
- (iii) $\mathbb{Z}[\xi]$ é o anel dos inteiros de $\mathbb{Q}(\xi)$.

Proposição 2.5.1 *Sejam p um número primo ímpar e ξ uma raiz p -ésima da unidade. Então, $D(1, \xi, \dots, \xi^{p-2}) = \pm p^{p-2}$.*

Demonstração: Pelo Teorema 2.5.3, temos que $\{1, \xi, \dots, \xi^{p-2}\}$ é uma base integral e que $f(X) = X^{p-1} + X^{p-2} + \dots + X + 1$ é o polinômio ciclotômico. Pela Proposição 2.4.4, temos que $D(1, \xi, \dots, \xi^{p-1}) = (-1)^{\frac{(p-1)(p-2)}{2}} \mathcal{N}(f'(\xi))$. Como p é ímpar temos que $\mathcal{N}(1, \xi, \dots, \xi^{p-1}) = (-1)^{\frac{p-1}{2}} \mathcal{N}(f'(\xi))$. Além disso, $f(X) = \frac{X^p - 1}{X - 1}$, e então $f'(X) = \frac{(X - 1)pX^{p-1} - (X^p - 1)}{(X - 1)^2}$. Assim, $f'(\xi) = \frac{(\xi - 1)p\xi^{p-1}}{(\xi^2 - 1)^2} = \frac{p\xi^{p-1}}{\xi - 1}$. Como $\mathcal{N}(f'(\xi)) = \frac{\mathcal{N}(p)\mathcal{N}(\xi)^{p-1}}{\mathcal{N}(\xi - 1)} = \frac{p^{p-1}(-1)^{p-1}}{p(-1)^{p-1}}$, segue que $D(1, \xi, \dots, \xi^{p-1}) = \frac{(-1)^{\frac{p-1}{2}} p^{p-1} (-1)^{p-1}}{p(-1)^{p-1}} = \pm p^{p-2}$. $\blacksquare$

Exemplo 2.5.1 Seja $K = \mathbb{Q}[\xi]$, com $\xi = e^{2\pi i/3}$. Temos que ξ é uma raiz 3-ésima da unidade do polinômio $f(X) = X^3 - 1$, então $D(1, \xi, \xi^2) = \pm 3^{3-2} = 3$. $\blacksquare$

2.6 Anéis Noetherianos

Nesta seção veremos o conceito de módulos e anéis Noetherianos enfocando suas principais propriedades.

Definição 2.6.1 Seja A um anel. Um A -módulo E é chamado Noetheriano se E satisfaz uma das condições do Teorema 1.1.2. Um anel A é chamado Noetheriano se, considerado como um A -módulo, é um módulo Noetheriano.

Exemplo 2.6.1 Todo anel principal é Noetheriano, uma vez que seus ideais são submódulos finitamente gerados. $\blacksquare$

Exemplo 2.6.2 O anel dos inteiros de um corpo de números é um anel Noetheriano. $\blacksquare$

Proposição 2.6.1 Sejam A um anel, E um A -módulo, e E' um submódulo de E . Então E é Noetheriano se, e somente se, E' e E/E' são Noetherianos.

Demonstração: Suponhamos que E é Noetheriano. Seja $(E_n)_{n \geq 0}$ uma seqüência crescente de submódulos de E' , que também é uma seqüência de submódulos de E . Como E é Noetheriano, segue que existe E_{n_0} elemento maximal da seqüência $(E_n)_{n \geq 0}$. Portanto E' é Noetheriano. Para mostrarmos que E/E' é Noetheriano, sejam $S = \{\text{conjunto dos submódulos de } E \text{ contendo } E'\}$ e $S' = \{\text{conjunto dos submódulos de } E/E'\}$. Assim, existe uma aplicação

bijetora $\varphi : S \rightarrow S'$ definida por $\varphi(H) = \phi(H)$ onde $\phi : E \rightarrow E/E'$ é o homomorfismo canônico. A inversa de φ é dada por $\theta : S' \rightarrow S$, onde $\theta(H') = \phi^{-1}(H')$. Através do isomorfismo ϕ temos que E/E' também é Noetheriano, uma vez que se $(H'_n)_{n \geq 0}$ é uma seqüência crescente de submódulos de E/E' , então $(\theta(H'_n))_{n \geq 0}$ é uma seqüência crescente de submódulos de E e como E é Noetheriano, segue que $(\theta(H'_n))_{n \geq 0}$ é estacionária, o que implica que $(H'_n)_{n \geq 0}$ é estacionária, ou seja, E/E' é Noetheriano. Reciprocamente, suponha que E' e E/E' são Noetherianos. Seja $(F_n)_{n \geq 0}$ uma seqüência crescente de submódulos de E . Como E' é Noetheriano, segue que a seqüência $(E' \cap F_n)_{n \geq 0}$ é estacionária, e como E/E' é Noetheriano, segue que a seqüência $\left(\frac{F_n + E'}{E'}\right)_{n \geq 0}$ é estacionária. Assim, a seqüência $(F_n + E')$ é estacionária e portanto (E_n) é estacionária, ou seja, E é Noetheriano. $\blacksquare$

Corolário 2.6.1 *Sejam A um anel e seja $E_1, \dots, E_n$ A -módulos Noetherianos. Então, o A -módulo $\prod_{i=1}^n E_i$ é Noetheriano.*

Demonstração: Faremos a prova por indução sobre n . Para $n = 2$ identificando $E_1 \simeq E_1 \times \{0\} \subseteq E_1 \times E_2$ e $E_2 \times \{0\} \subseteq E_1 \times E_2$, temos que $\frac{E_1 \times E_2}{E_1 \times \{0\}}$ é isomorfo a E_2 . Como E_2 e $E_1 \times \{0\}$ são Noetherianos, segue da Proposição 2.6.1 que $E_1 \times E_2$ é Noetheriano. Agora, suponha por hipótese de indução que $E = E_1 \times E_2 \times \dots \times E_{n-1}$ é Noetheriano. Como E_n é Noetheriano, segue do caso $n = 2$ que $E = E_1 \times E_2 \times \dots \times E_n$ é Noetheriano. $\blacksquare$

Corolário 2.6.2 *Seja A um anel Noetheriano e seja E um A -módulo finitamente gerado. Então E é um módulo Noetheriano.*

Demonstração: Seja $\{e_1, \dots, e_n\}$ um conjunto de geradores de E sobre A . Assim, a aplicação $\varphi : A^n \rightarrow E$ definida por $\varphi(a_1, a_2, \dots, a_n) = \sum_{i=1}^n a_i e_i$ é um homomorfismo sobrejetor e que $A^n / \ker(\varphi)$ é isomorfo a E . Pelo Corolário 2.6.1 temos que A^n é Noetheriano, e da Proposição 2.6.1, segue que $\ker(\varphi)$ e E são Noetherianos. $\blacksquare$

Proposição 2.6.2 *Sejam A um anel Noetheriano integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau finito e A' o fecho inteiro de A em $\mathbb{L}$. Suponha $\mathbb{K}$ de característica zero. Então A' é um A -módulo finitamente gerado e um anel Noetheriano.*

Demonstração: Segue do Teorema 2.4.1 que A' é um A -submódulo de um A módulo livre de posto n , e portanto A' é um A -módulo finitamente gerado. Pelo Corolário 2.6.2, temos

que A' é um A -módulo Noetheriano. Como os ideais de A' são A -submódulos de A' , segue que satisfazem as condições de maximalidade do Teorema 1.1.2. Portanto, A' é um anel Noetheriano. $\blacksquare$

Proposição 2.6.3 *Sejam A um anel, B um subanel de A e $\mathfrak{p}$ um ideal primo de A . Então $\mathfrak{p} \cap B$ é um ideal primo de B .*

Demonstração: Sejam os seguintes homomorfismos $B \xrightarrow{i} A \xrightarrow{\pi} \frac{A}{\mathfrak{p}}$, onde i a inclusão e π a projeção, e seja o homomorfismo $\theta = \pi \circ i : B \rightarrow A/\mathfrak{p}$, definido por $\theta(b) = b + \mathfrak{p}$, $\forall b \in B$. Temos que θ é um homomorfismo, pois é uma composição de homomorfismos. Temos que $\text{Ker}(\theta) = B \cap \mathfrak{p}$, uma vez que se $x \in \text{Ker}(\theta) \Rightarrow x \in B$ e $\theta(x) = \bar{0} \Rightarrow x \in B$ e $b + \mathfrak{p} = \bar{0} \Rightarrow x \in B$ e $b \in \mathfrak{p} \Rightarrow x \in B \cap \mathfrak{p}$, ou seja, $\text{Ker}(\theta) \subset B \cap \mathfrak{p}$. Por outro lado, se $y \in B \cap \mathfrak{p} \Rightarrow y \in \mathfrak{p}$ e $y \in B \Rightarrow \theta(y) = (\pi \circ i)(y) = \pi(y) = y + \mathfrak{p} \stackrel{y \in \mathfrak{p}}{=} \bar{0} \Rightarrow y \in \text{Ker}(\theta)$, ou seja, $B \cap \mathfrak{p} \subset \text{Ker}(\theta)$. Logo, $\text{Ker}(\theta) = B \cap \mathfrak{p}$. Portanto, pelo Teorema 1.1.1, temos que $B/B \cap \mathfrak{p} \simeq \text{Im}(\theta) \subset A/\mathfrak{p}$. Como $A/\mathfrak{p}$ é domínio, segue que $\text{Im}(\theta)$ é um domínio, e portanto $B/B \cap \mathfrak{p}$ é um domínio, e portanto $B \cap \mathfrak{p}$ é um ideal primo. $\blacksquare$

Proposição 2.6.4 *Se um ideal primo $\mathfrak{p}$ de um anel A contém um produto $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ de ideais, então $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$.*

Demonstração: Se $\mathfrak{a}_i \not\subset \mathfrak{p}, \forall i = 1, \dots, n$, então existe um elemento $a_i \in \mathfrak{a}_i - \mathfrak{p}$, para todo $i = 1, \dots, n$. Como $\mathfrak{p}$ é primo, temos que $a_1 \cdots a_n \notin \mathfrak{p}$. Por outro lado, temos que $a_1 \cdots a_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{p}$, o que é um absurdo uma vez que $a_i \notin \mathfrak{p}, \forall i = 1, \dots, n$. Portanto, $\mathfrak{a}_i \subset \mathfrak{p}$, para algum $i = 1, \dots, n$. $\blacksquare$

Proposição 2.6.5 *Seja A um domínio Noetheriano, então todo ideal não nulo de A contém um produto de ideais primos não nulos de A .*

Demonstração: Sendo A Noetheriano, seus ideais são A -módulos Noetherianos. Seja F o conjunto de todos os ideais não nulos de A que não contém um produto de ideais primos não nulos de A . Se $F \neq \emptyset$, então como A é Noetheriano, temos que F possui um elemento maximal M . Temos que M não é primo, pois caso contrário não pertenceria a F . Além disso, $M \neq A$. Por M não ser um ideal primo, existem elementos $x, y \in A - M$, tal que $xy \in M$. Os ideais $M + Ax$ e $M + Ay$ contém M propriamente e pela maximalidade de M estes ideais não estão em

F , assim existem ideais $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ primos não nulos de A , tais que $M + Ax \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ e $M + Ay \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Assim, $M \supset (M + Ax)(M + Ay) \supset M + Axy \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s$, o que é um absurdo. Assim, $F = \emptyset$. Portanto, todo ideal não nulo de A contém um produto de ideais não nulos. $\blacksquare$

Corolário 2.6.3 *Se A é um anel Noetheriano, então todo ideal de A contém um produto de ideais primos.* $\blacksquare$

Definição 2.6.2 *Sejam A um domínio e K seu corpo de frações. Um A -submódulo I de K é chamado um **ideal fracionário** de A se existe um $d \in A - (0)$, tal que $d \cdot I \subset A$.*

Segue da definição que os elementos de um ideal fracionário I têm um denominador comum $d \in A$, e quando $d = 1$, chamamos I de *ideal inteiro*. Todo A -submódulo I finitamente gerado de K é um ideal fracionário, uma vez que se $\{x_1, \dots, x_n\}$ é um conjunto finito de geradores de I , então os x_i 's têm um denominador comum d , ou seja, d é o produto dos denominadores d_i , onde $x_i = a_i d_i^{-1}$, com $a_i, d_i \in A$, e d é o denominador comum de I . Reciprocamente, se A é Noetheriano, todo ideal fracionário I é um A -módulo finitamente gerado, isto é, $I \subset d^{-1}A$ e $d^{-1}A$ sendo um A -módulo isomorfo a A é um módulo Noetheriano. O produto II' de dois ideais fracionários I e I' é definido como o conjunto das somas $\sum_i x_i y_i$ com $x_i \in I$ e $y_i \in I'$. Se os ideais I e I' são ideais fracionários com denominadores comum d e d' , então os conjuntos $I \cap I'$, $I + I'$ e II' são ideais fracionários, que são A -submódulos de K e tem denominadores comum d ou d' , dd' e dd' , respectivamente.

Definição 2.6.3 *Diz-se que uma operação $\star$ sobre um conjunto E , define uma estrutura de monóide sobre E ou que E é um monóide com relação a operação $\star$, se esta satisfaz a propriedade associativa e se em E possui um elemento neutro e .*

O conjunto dos naturais $\mathbb{N}$ é um monóide com a soma.

2.7 Anéis de Dedekind

Nesta seção apresentamos o conceito de anéis de Dedekind, onde veremos que nestes anéis vale a fatoração única de ideais em um produto de ideais primos.

Definição 2.7.1 Um anel A é chamado um anel de Dedekind, se A é Noetheriano, integralmente fechado e se todo ideal primo não nulo de A é maximal.

Exemplo 2.7.1 Todo anel principal, em particular o anel $\mathbb{Z}$, é um anel de Dedekind, uma vez que é integralmente fechado, Noetheriano e que todo ideal primo é maximal. ■

Teorema 2.7.1 Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de grau finito de $\mathbb{K}$ e A' o fecho inteiro de A em $\mathbb{L}$. Então, A' é um anel de Dedekind e um A -módulo finitamente gerado.

Demonstração: Temos que A' é integralmente fechado e pela Proposição 2.6.2 temos que A' é um A -módulo finitamente gerado e é Noetheriano. Resta mostrarmos que todo ideal primo $\mathfrak{p}' \neq (0)$ de A' é maximal. Seja $x \in \mathfrak{p}' - (0)$ e seja a equação de dependência inteira de x sobre A dada por $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ com $a_i \in A$ cujo o grau é mínimo. Assim, $a_0 \neq 0$, pois caso contrário obteríamos uma equação de grau menor. Portanto, temos que $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$, ou seja, $\mathfrak{p}' \cap A \neq (0)$. Pela Proposição 2.6.3 temos que $\mathfrak{p}' \cap A$ é um ideal primo de A , e como A é Dedekind, segue que $\mathfrak{p}' \cap A$ é um ideal maximal de A , e portanto, $A/\mathfrak{p}' \cap A$ é um corpo. Além disso, $A/\mathfrak{p}' \cap A$ pode ser identificado com um subanel de $A'/\mathfrak{p}'$, e como A' é inteiro sobre A , segue que $A'/\mathfrak{p}'$ é inteiro sobre $A/\mathfrak{p}' \cap A$. Daí, pela Proposição 2.1.3 temos que $A'/\mathfrak{p}'$ é corpo, ou seja, $\mathfrak{p}'$ é maximal. ■

O anel dos inteiros de um corpo de números é um anel de Dedekind, mas que não é sempre um anel principal, como podemos ver no próximo exemplo.

Exemplo 2.7.2 Seja $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}]$ o anel dos inteiros de $\mathbb{Q}[\sqrt{-5}]$. Temos que $\mathcal{O}_{\mathbb{K}}$ não é fatorial, uma vez que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Além disso, $\mathcal{O}_{\mathbb{K}}$ não é principal. De fato, temos que $\mathcal{N}(1 + \sqrt{-5}) = \mathcal{N}(1 - \sqrt{-5}) = 6$, $\mathcal{N}(2) = 4$ e $\mathcal{N}(3) = 9$, e que $1 + \sqrt{-5}$ não possui um divisor não trivial em $\mathcal{O}_{\mathbb{K}}$, pois se $a + b\sqrt{-5}$ é um divisor não trivial de $1 + \sqrt{-5}$, ou seja, se $1 + \sqrt{-5} = (a + b\sqrt{-5})y$, com $y \in \mathcal{O}_{\mathbb{K}}$, $y \neq \pm 1$ e $y \neq 1 + \sqrt{-5}$, então $6 = \mathcal{N}(1 + \sqrt{-5}) = \mathcal{N}(a + b\sqrt{-5})\mathcal{N}(y)$ e que $\mathcal{N}(a + b\sqrt{-5})$ seria um divisor não trivial de 6, mas isto é impossível, pois $a^2 + 5b^2 = 2$ e $a^2 + 5b^2 = 3$, não possui solução em $\mathbb{Z}$. Agora, se $\mathcal{O}_{\mathbb{K}}$ for principal, então o elemento primo $1 + \sqrt{-5}$, que divide o produto $2 \cdot 3$, deveria dividir 2 ou 3. Assim, tomando as normas, segue que 6 divide 4 ou 9, o que não acontece. Portanto, $\mathcal{O}_{\mathbb{K}}$ não é principal. ■

O exemplo anterior mostra que no anel dos inteiros $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ não vale a fatoração única de elementos em produto de fatores primos, ou seja, $\mathcal{O}_K$ não é um anel fatorial, e que também não é principal. Em anéis de Dedekind existe uma elegante generalização desta propriedade, ou seja, em um anel de Dedekind, os ideais fatoram-se unicamente em produto de ideais primos, e decorre desta propriedade resultados importantes.

Lema 2.7.1 *Seja A um domínio de Dedekind que não é um corpo e seja K seu corpo de frações. Seja $\mathfrak{m}$ um ideal maximal de A . Então, $\mathfrak{m}' = \{x \in K : x\mathfrak{m} \subset A\}$ é um ideal fracionário de K .*

Demonstração: Como A não é um corpo, temos que $\mathfrak{m} \neq \{0\}$ e que $\mathfrak{m}' \neq \emptyset$, pois $0 \in \mathfrak{m}'$. Sejam $x, y \in \mathfrak{m}'$. Então pela definição de $\mathfrak{m}'$, temos que $x\mathfrak{m} \subset A$ e $y\mathfrak{m} \subset A$, e portanto, $(x+y)\mathfrak{m} = x\mathfrak{m} + y\mathfrak{m} \subset A$, ou seja, $x+y \in \mathfrak{m}'$. Agora, sejam $x \in \mathfrak{m}'$ e $a \in A$. Assim, $x\mathfrak{m} \subset A$, e portanto, $(xa)\mathfrak{m} = a(x\mathfrak{m}) \subset A$, ou seja, $xa \in \mathfrak{m}'$. Finalmente, temos que $d\mathfrak{m} \subset A$, para todo $d \in A - \{0\}$, ou seja, $\mathfrak{m}'$ é um ideal fracionário de K . $\blacksquare$

Teorema 2.7.2 *Seja A um anel de Dedekind que não é um corpo e seja K seu corpo de frações. Todo ideal maximal de A é invertível no monóide dos ideais fracionários de A .*

Demonstração: Seja $\mathfrak{m}$ um ideal maximal de A . Pelo Lema 2.7.1 temos que $\mathfrak{m}' = \{x \in K : x\mathfrak{m} \subset A\}$ é um ideal fracionário de K . Pela definição de $\mathfrak{m}'$, segue que $\mathfrak{m}'\mathfrak{m} \subset A$, e como $\mathfrak{m}$ é um ideal de A , segue que $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{m}\mathfrak{m}' \subset A$. Como $\mathfrak{m}$ é maximal, temos que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ ou $\mathfrak{m}\mathfrak{m}' = A$. Vamos mostrar que $\mathfrak{m}\mathfrak{m}' \neq \mathfrak{m}$. Para isto suponhamos que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. Seja $x \in \mathfrak{m}'$. Então, por indução sobre n temos que $x^n\mathfrak{m} \subset A$, para todo $n \in \mathbb{N}$, ou seja, $dx^n \in A$, $\forall d \in A$ e $\forall n \in \mathbb{N}$. Assim, $A[x]$ é um ideal fracionário de A , e como A é Noetheriano, segue que $A[x]$ é um A -módulo finitamente gerado. Portanto, x é inteiro sobre A , e como A é integralmente fechado, segue que $x \in A$, ou seja, $\mathfrak{m}' \subset A$. Como $A \subset \mathfrak{m}'$, segue que $A = \mathfrak{m}'$. Por outro lado, seja $a \in \mathfrak{m}$. Pela Proposição 2.6.5, segue que o ideal aA contém um produto de ideais primos não nulos $\mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$, com n o menor possível. Assim, $\mathfrak{m} \supset aA \supset \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$. Pela Proposição 2.6.4, temos que $\mathfrak{m}$ contém um dos $\mathfrak{p}_i$'s, que sem perda de generalidade, digamos que seja $\mathfrak{p}_1$, ou seja $\mathfrak{m} \supset \mathfrak{p}_1$. Como A é Dedekind, segue que $\mathfrak{p}_1 = \mathfrak{m}$, pois $\mathfrak{p}_1$ é maximal. Agora, seja $\mathfrak{b} = \mathfrak{p}_2 \dots \mathfrak{p}_n$. Então, $Aa \supset \mathfrak{m}\mathfrak{b}$ e $Aa \not\supset \mathfrak{b}$ pela minimalidade de n . Assim, existe $y \in \mathfrak{b}$, tal que $y \notin Aa$. Como $\mathfrak{m}\mathfrak{b} \subset Aa$, segue que $my \subset Aa$, ou seja, $mya^{-1} \subset A$. Pela

definição de $\mathfrak{m}'$, segue que $ya^{-1} \in \mathfrak{m}'$. Como $y \notin Aa$, segue que $ya^{-1} \notin A$, ou seja, $\mathfrak{m}' \neq A$, o que é um absurdo, pois já tínhamos que $\mathfrak{m}' = A$. Portanto, $\mathfrak{m}\mathfrak{m}' = A$. $\blacksquare$

Teorema 2.7.3 *Sejam A um domínio de Dedekind e $\mathfrak{a} \neq A$ um ideal não nulo de A . Então, existem ideais primos não nulos $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ de A e inteiros positivos $e_1, \dots, e_g$, tal que $\mathfrak{a} = \prod_{i=1}^g \mathfrak{p}_i^{e_i}$, e esta expressão é única.*

Demonstração: Pela Proposição 2.6.5, existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ não nulos de A , tal que $\mathfrak{p}_1, \dots, \mathfrak{p}_s \subset \mathfrak{a}$. Provemos que $\mathfrak{a}$ é um produto de ideais primos não nulos de A por indução sobre s . Se $s = 1$, temos $\mathfrak{a} \supset \mathfrak{p}_1$, mas como $\mathfrak{p}_1$ é um ideal maximal, pois A é Dedekind, então $\mathfrak{a} = \mathfrak{p}_1$, ou seja, $\mathfrak{a}$ é primo. Agora suponhamos que todo ideal não nulo de A que contém um produto de $s - 1$ ideais primos não nulos de A é um produto de ideais primos de A . Temos que $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{m}$ na coleção dos ideais não triviais de A que contém $\mathfrak{a}$. Seja $\mathfrak{m}^{-1}$ o ideal fracionário inverso de $\mathfrak{m}$. Como $\mathfrak{m} \supset \mathfrak{a} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_s$, segue da Proposição 2.6.4, que $\mathfrak{m}$ contém um dos $\mathfrak{p}_i$'s, $i = 1, \dots, s$, e sem perda de generalidade digamos que $\mathfrak{m} \supset \mathfrak{p}_s$. Como $\mathfrak{p}_s$ é maximal, segue que $\mathfrak{p}_s = \mathfrak{m}$. Assim, $\mathfrak{p}_1 \cdots \mathfrak{p}_{s-1} \subset \mathfrak{a}\mathfrak{m}^{-1} \subset \mathfrak{m}\mathfrak{m}^{-1} = A$. Da hipótese de indução decorre que $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_t$, com $\mathfrak{q}_j$'s; $j = 1, \dots, t$, ideais primos não nulos de A , e portanto $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_t \mathfrak{p}_s$, como queríamos. Para a unicidade, suponhamos que, $\prod_{i=1}^g \mathfrak{p}_i^{e_i} = \prod_{i=1}^h \mathfrak{p}_i^{f_i}$. Então, $A = \prod \mathfrak{p}_i^{e_i - f_i}$. Se $e_i - f_i \neq 0$, podemos separar os expoentes positivos e os expoentes negativos e reescrevê-los como, $\mathfrak{p}_1^{\alpha_1} \mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_s^{\beta_s}$, com $\mathfrak{p}_i, \mathfrak{q}_j$ ideais primos não nulos de A e $\alpha_i, \beta_j > 0$ e $\mathfrak{p}_i \neq \mathfrak{q}_j, \forall i, j$. Temos que $\mathfrak{p}_1$ contém $\mathfrak{q}_1 \cdots \mathfrak{q}_s$ e pela Proposição 2.6.4, segue que $\mathfrak{p}_1 \supset \mathfrak{q}_j$, para algum j . Suponhamos sem perda de generalidade, que $\mathfrak{p}_1 \supset \mathfrak{q}_1$, mas $\mathfrak{p}_1$ e $\mathfrak{q}_1$ são ideais maximais, logo $\mathfrak{p}_1 = \mathfrak{q}_1$, o que é uma contradição. $\blacksquare$

Segue dos Teoremas 2.7.2 e 2.7.3 o seguinte corolário.

Corolário 2.7.1 *Seja A um anel de Dedekind. O monóide dos ideais fracionários de A é um grupo, que denotaremos por $I(A)$.* $\blacksquare$

Seja A um anel de Dedekind. Os ideais fracionários principais de A , isto é, aqueles da forma Ax , com $x \in \mathbb{K}^*$, formam um subgrupo $F(A)$ de $I(A)$, uma vez que $(Ax)(Ay)^{-1} = Axy^{-1}$. O grupo quociente $C(A) = I(A)/F(A)$ é chamado **grupo das classes dos ideais de A** .

Observação 2.7.1 Para que A seja um anel principal, é necessário e suficiente, que $C(A)$ consista de apenas um elemento. $\blacksquare$

Definição 2.7.2 Sejam A um anel de Dedekind e $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A . Dizemos que $\mathfrak{a}$ divide $\mathfrak{b}$, e denotamos por $\mathfrak{a}|\mathfrak{b}$, se existe um ideal $\mathfrak{c}$ em A tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$. Assim $\mathfrak{a}$ divide $\mathfrak{b}$ se, e somente se, $\mathfrak{a} \supset \mathfrak{b}$.

2.8 Norma de um ideal

Consideraremos nesta seção K um corpo de números de grau n e $\mathcal{O}_K$ o anel dos inteiros de K .

Definição 2.8.1 Seja $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Denotamos por $\mathcal{N}_{\mathcal{O}_K}(\mathfrak{a})$ e chamamos de **norma do ideal $\mathfrak{a}$** , o número (cardinal) dos elementos do anel quociente $\mathcal{O}_K/\mathfrak{a}$, isto é, $\mathcal{N}(\mathfrak{a}) = \#(\mathcal{O}_K/\mathfrak{a})$.

Observação 2.8.1 Quando não houver dúvida quanto ao anel A , que contém o ideal $\mathfrak{a}$, usaremos a notação $\mathcal{N}(\mathfrak{a})$ ao invés de $\mathcal{N}_{\mathcal{O}_K}(\mathfrak{a})$. $\blacksquare$

Exemplo 2.8.1 Seja $\mathfrak{a} = \langle 2 - i \rangle$ um ideal principal de $\mathbb{Z}[i]$, e seja o anel quociente $\frac{\mathbb{Z}[i]}{\mathfrak{a}} = \{x + \mathfrak{a} ; x \in \mathbb{Z}[i]\}$. A norma de $\mathfrak{a}$ é o número de classes laterais de $\mathfrak{a}$. Como $2 - i \equiv 0 \pmod{\mathfrak{a}}$ temos que $2 \equiv i \pmod{\mathfrak{a}}$, e então para $x = a + bi$, com $a, b \in \mathbb{Z}$, temos que $x = a + bi \equiv a + 2b \pmod{\mathfrak{a}}$. Visto que $(2 + i)(2 - i) = 5 \in \mathfrak{a}$, segue que as classes laterais de $\mathfrak{a}$ em $\mathbb{Z}[i]$ são $\{0, 1, 2, -1, -2\}$, ou seja, $\mathcal{N}(\mathfrak{a}) = 5$. $\blacksquare$

Proposição 2.8.1 Se $x \in \mathcal{O}_K$, $x \neq 0$, então $|\mathcal{N}(x)| = \#\mathcal{O}_K/\mathcal{O}_Kx$.

Demonstração: Seja $x \in \mathcal{O}_K$, $x \neq 0$. Então, pelo Corolário 2.3.1, temos que $\mathcal{N}(x) \in \mathbb{Z}$. Pelo Corolário 2.4.2 temos que $\mathcal{O}_K$ é um $\mathbb{Z}$ -módulo livre de posto n . Além disso, como $\psi : \mathcal{O}_K \rightarrow \mathcal{O}_Kx$ definido por $\psi(a) = ax$, com $a \in \mathcal{O}_K$, é um isomorfismo, segue que $\mathcal{O}_Kx$ é um $\mathbb{Z}$ -submódulo livre de posto n de $\mathcal{O}_K$. Pelo Teorema 1.1.3, existe uma base $\{e_1, e_2, \dots, e_n\}$ do $\mathbb{Z}$ -módulo $\mathcal{O}_K$ e elementos $c_i \in \mathbb{N}$, tal que $\{c_1e_1, c_2e_2, \dots, c_ne_n\}$ é uma base de $\mathcal{O}_Kx$. Além disso, temos que o grupo abeliano $\mathcal{O}_K/\mathcal{O}_Kx$ é isomorfo ao grupo abeliano $\prod_{i=1}^n \mathbb{Z}/c_i\mathbb{Z}$, cuja

ordem é $c_1 c_2 \dots c_n$. Seja a aplicação linear $\varphi : \mathcal{O}_K \rightarrow \mathcal{O}_K x$ definida por $\varphi(e_i) = c_i e_i$, com $i = 1, \dots, n$. Temos que $\det(\varphi) = c_1 c_2 \dots c_n$. Por outro lado, como $\{x e_1, \dots, x e_n\}$ também é uma base de $\mathcal{O}_K x$, existe um automorfismo de $\mathbb{Z}$ -módulo $\phi : \mathcal{O}_K x \rightarrow \mathcal{O}_K x$, definido por $\phi(c_i e_i) = x e_i$, $i = 1, \dots, n$. Assim, como o $\det(\phi) \in \mathbb{Z}$ é invertível, segue que $\det(\phi) = \pm 1$. Mas o homomorfismo $\phi\varphi$ é a multiplicação por x , e seu determinante por definição é a $\mathcal{N}(x)$. Portanto, como $\det(\phi\varphi) = \det(\phi)\det(\varphi)$, segue que $\mathcal{N}(x) = \pm c_1 \dots c_n = \pm \#(\mathcal{O}_K/\mathcal{O}_K x)$. $\blacksquare$

Proposição 2.8.2 *Seja $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Então, $\mathcal{N}(\mathfrak{a})$ é finita.*

Demonstração: Seja $x \in \mathfrak{a}$, um elemento não nulo. Então $\mathcal{O}_K x \subset \mathfrak{a}$. Assim, $\frac{\mathcal{O}_K}{\mathfrak{a}}$ pode ser visto como um subconjunto de $\frac{\mathcal{O}_K}{\mathcal{O}_K x}$. Daí, $\# \frac{\mathcal{O}_K}{\mathfrak{a}} \leq \# \frac{\mathcal{O}_K}{\mathcal{O}_K x}$, que é finito pela Proposição 2.8.1. Portanto, $\mathcal{N}(\mathfrak{a}) = \# \frac{\mathcal{O}_K}{\mathfrak{a}}$ é finita. $\blacksquare$

Proposição 2.8.3 *Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathcal{O}_K$, então $\mathcal{N}(\mathfrak{a}\mathfrak{b}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.*

Demonstração: Pelo Teorema 2.7.3, temos que $\mathfrak{b} = \prod_{i \in I} \mathfrak{p}_i^{\alpha_i}$, onde os $\mathfrak{p}_i$'s são ideais primos de $\mathcal{O}_K$. Como $\mathcal{O}_K$ é um domínio de Dedekind, então os ideais $\mathfrak{p}_i$'s, com $i \in I$ são ideais maximais. Seja $\mathfrak{p}_i = \mathfrak{m}$, para algum $i \in I$. Por indução sobre o número de fatores, é suficiente provar que

$$\mathcal{N}(\mathfrak{a}\mathfrak{m}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{m}), \quad (2.8.5)$$

onde $\mathfrak{m}$ é um ideal maximal de $\mathcal{O}_K$, ou seja devemos mostrar que

$$\# \left(\frac{\mathcal{O}_K}{\mathfrak{a}\mathfrak{m}} \right) = \# \left(\frac{\mathcal{O}_K}{\mathfrak{a}} \right) \cdot \# \left(\frac{\mathcal{O}_K}{\mathfrak{m}} \right). \quad (2.8.6)$$

Agora, como $\mathfrak{a}\mathfrak{m} \subset \mathfrak{a}$, temos que o homomorfismo sobrejetor $\phi : \mathcal{O}_K/\mathfrak{a}\mathfrak{m} \rightarrow \mathcal{O}_K/\mathfrak{a}$, definido por $\phi(x + \mathfrak{a}\mathfrak{m}) = x + \mathfrak{a}$, para $x \in \mathcal{O}_K$, possui $\text{Ker}\phi = \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$. Pelo Teorema 1.1.1 temos que $\frac{\mathcal{O}_K}{\mathfrak{a}\mathfrak{m}} / \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \simeq \mathcal{O}_K/\mathfrak{a}$. Logo,

$$\# \left(\frac{\mathcal{O}_K}{\mathfrak{a}\mathfrak{m}} \right) = \# \left(\frac{\mathcal{O}_K}{\mathfrak{a}} \right) \cdot \# \left(\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \right). \quad (2.8.7)$$

Assim, de (2.8.6) e (2.8.7) podemos concluir que (2.8.5) é verificado se $\# \left(\frac{\mathcal{O}_K}{\mathfrak{m}} \right) = \# \left(\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} \right)$.

Agora temos que $\frac{\mathfrak{a}}{\mathfrak{am}}$ é um espaço vetorial sobre $\frac{\mathcal{O}_K}{\mathfrak{m}}$, e os $\mathcal{O}_K$ -submódulos são ideais de $\frac{\mathfrak{a}}{\mathfrak{am}}$ e são do tipo $\frac{\mathfrak{b}}{\mathfrak{am}}$, onde $\mathfrak{b}$ é um ideal, tal que $\mathfrak{am} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Mas, como todo ideal fracionário num domínio de Dedekind admite inverso, temos que $\mathfrak{a}^{-1}\mathfrak{am} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \xrightarrow{\mathfrak{a}^{-1}\mathfrak{a}=\mathcal{O}_K} \mathfrak{m} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K$. $\mathfrak{m}$ é maximal $\Rightarrow \mathfrak{m} = \mathfrak{a}^{-1}\mathfrak{b}$ ou $\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_K \Rightarrow \mathfrak{am} = \mathfrak{b}$ ou $\mathfrak{b} = \mathfrak{a}$. Assim, os $\mathcal{O}_K$ -submódulos de $\frac{\mathfrak{a}}{\mathfrak{am}}$, ou os subespaços do espaço vetorial $\frac{\mathfrak{a}}{\mathfrak{am}}$ são apenas os triviais. Portanto, temos que $\dim_{\frac{\mathcal{O}_K}{\mathfrak{m}}} \frac{\mathfrak{a}}{\mathfrak{am}} = 1$, e portanto $\# \left(\frac{\mathcal{O}_K}{\mathfrak{m}} \right) = \# \left(\frac{\mathfrak{a}}{\mathfrak{am}} \right)$. $\square$

Seja $\mathfrak{p} \subset \mathcal{O}_K$ um ideal primo. Pela Proposição 2.6.3 temos que $\mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$ é um ideal primo de $\mathbb{Z}$, onde $p \in \mathbb{Z}$ é um número primo. Sejam os homomorfismos $\mathbb{Z} \xrightarrow{i} A \xrightarrow{\pi} \mathcal{O}_K/\mathfrak{p}$, onde i é a inclusão e π a projeção. Temos que $\text{Ker}(\pi \circ i) = \mathfrak{p} \cap \mathbb{Z} = \langle p \rangle$. Assim, pelo Teorema 1.1.1, temos que $\mathbb{Z}/\langle p \rangle \simeq \text{Im}(\pi \circ i)$. Assim, $\mathcal{O}_K/\mathfrak{p}$ (corpo) pode ser visto como um espaço vetorial sobre $\mathbb{Z}/\langle p \rangle$, cuja dimensão é chamada **grau de inércia** de $\mathfrak{p}$.

Proposição 2.8.4 a) Para todo ideal primo não nulo $\mathfrak{p}$ de $\mathcal{O}_K$ temos que $\mathcal{N}(\mathfrak{p}) = p^f$, onde f é o grau de inércia de $\mathfrak{p}$ e p é o único número primo em $\mathfrak{p}$.

b) Para todo ideal não nulo $\mathfrak{a}$ temos que $\mathcal{N}(\mathfrak{a}) = 1$ se, e somente se, $\mathfrak{a} = \mathcal{O}_K$.

c) Se $\mathcal{N}(\mathfrak{a})$ for um número primo, então o ideal $\mathfrak{a}$ é primo.

d) $\mathcal{N}(\mathfrak{a})$ é um elemento de $\mathfrak{a}$.

e) Se $\mathfrak{a}$ for um múltiplo do ideal $\mathfrak{b}$ e $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})$ então $\mathfrak{a} = \mathfrak{b}$.

Demonstração: a) Segue do fato que $\mathcal{O}_K/\mathfrak{p}$ é um $\mathbb{Z}/p\mathbb{Z}$ -espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$ de dimensão f , ou seja, $\mathcal{N}(\mathfrak{p}) = \# \left(\frac{\mathcal{O}_K}{\mathfrak{p}} \right) = p^f$.

b) Se $\mathcal{N}(\mathfrak{a}) = 1 \iff \#(\mathcal{O}_K/\mathfrak{a}) = 1 \iff \mathcal{O}_K = \mathfrak{a}$.

c) Suponhamos que $\mathfrak{a}$ não seja um ideal primo. Então, $\mathfrak{a} = \mathcal{O}_K$ ou $\mathfrak{a} = \mathfrak{bc}$, onde $\mathfrak{b}$ e $\mathfrak{c}$ são ideais não nulos e distintos de $\mathcal{O}_K$. Assim, temos:

i) Se $\mathfrak{a} = \mathcal{O}_K$, então $\mathcal{N}(\mathfrak{a}) = 1$, que é contra a hipótese.

ii) Se $\mathfrak{a} = \mathfrak{bc}$, então temos $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})\mathcal{N}(\mathfrak{c})$ e como por hipótese $\mathcal{N}(\mathfrak{a}) = p$, onde p é um número primo, então $\mathcal{N}(\mathfrak{b}) = 1$ e $\mathcal{N}(\mathfrak{c}) = p$ ou $\mathcal{N}(\mathfrak{b}) = p$ e $\mathcal{N}(\mathfrak{c}) = 1$. Porém, se isso ocorrer temos por (b), que $\mathfrak{b} = \mathcal{O}_K$ ou $\mathfrak{c} = \mathcal{O}_K$, o que é contra a hipótese. Portanto, $\mathfrak{a}$ é um ideal primo.

d) Temos que $(\mathcal{O}_K/\mathfrak{a}, +)$ é um grupo aditivo, tal que sua ordem é $\mathcal{N}(\mathfrak{a}) = m$. Assim, $m \cdot \bar{1} = \bar{0}$, onde 1 é unidade de $\mathcal{O}_K$ e $\bar{0}$ o elemento neutro do anel $\mathcal{O}_K/\mathfrak{a}$. Logo, $m \in \mathfrak{a}$, ou seja, $\langle m \rangle \subseteq \mathfrak{a}$.

e) Se $\mathfrak{a}$ é múltiplo do ideal $\mathfrak{b}$, então existe um ideal $\mathfrak{c}$ de $\mathcal{O}_K$, tal que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Assim, $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})\mathcal{N}(\mathfrak{c})$. Por hipótese, como $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{b})$, segue que, $\mathcal{N}(\mathfrak{c}) = 1$. Logo, $\mathfrak{c} = \mathcal{O}_K$ e $\mathfrak{a} = \mathfrak{b}$. ▀

Proposição 2.8.5 *Para todo $m \in \mathbb{N} \setminus \{0\}$ existe somente um número finito de ideais não nulos $\mathfrak{a}$ de $\mathcal{O}_K$ tais que $\mathcal{N}(\mathfrak{a}) = m$.*

Demonstração: Pelo Teorema 2.7.1 sabemos que o anel dos inteiros $\mathcal{O}_K$ é um domínio de Dedekind. Seja $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Então, provemos que o conjunto de todos os ideais não nulos de $\mathcal{O}_K$ que contém $\mathfrak{a}$ é finito. Pelo Teorema 2.7.3, temos que o ideal $\mathfrak{a}$ pode ser escrito como um produto de ideais primos não nulos de $\mathcal{O}_K$, ou seja, $\mathfrak{a} = \mathfrak{p}_1^{k_1} \dots \mathfrak{p}_k^{k_s}$, onde $k_1, \dots, k_s \in \mathbb{N}$ e $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ são ideais primos não nulos de $\mathcal{O}_K$. Assim, temos que $\mathfrak{a}$ possui um número finito de ideais não nulos de $\mathcal{O}_K$ que dividem $\mathfrak{a}$, ou seja, existem $l_1, \dots, l_t$, $t \leq s$, $l_i \leq k_i$, $\forall i$, tal que $\mathfrak{p}_1^{l_1} | \mathfrak{a}, \dots, \mathfrak{p}_t^{l_t} | \mathfrak{a}$. Portanto, existe um número finito de ideais que contém $\mathfrak{a}$, isto é, o conjunto de todos os ideais não nulos de $\mathcal{O}_K$ que contém $\mathfrak{a}$ é finito, denotemos este por $I = \{\mathfrak{q}_i \text{ ideal de } \mathcal{O}_K : \mathfrak{q}_i \supseteq \mathfrak{a}\}$. Pela Proposição 2.8.4, temos que $\mathcal{N}(\mathfrak{a})$ é um elemento do ideal $\mathfrak{a}$, mas $\mathfrak{q}_i \supseteq \mathfrak{a}$, assim segue que $\mathcal{N}(\mathfrak{a})$ é um elemento de $\mathfrak{q}_i \in I$, e como I é finito, segue o resultado. ▀

2.9 Fatoração de um ideal em uma extensão

Sejam K um corpo numérico, $\mathcal{O}_K$ o anel dos inteiros de K , L uma extensão de K de grau finito n e $\mathcal{O}_L$ o anel dos inteiros de L .

Definição 2.9.1 *Sejam A um domínio, K seu corpo de frações e S um subconjunto não vazio de $A - (0)$ fechado sob a multiplicação com $1_A \in S$. Chamamos de **anel de frações com respeito a S** o conjunto de todos os elementos de K que são escritos na forma $\frac{a}{s}$ com $a \in A$ e $s \in S$. **Notação:** $S^{-1}A$.*

A seguir daremos algumas propriedades sobre os anéis de frações.

1. $S^{-1}A$ é um anel comutativo. De fato, $\forall x, y \in S^{-1}A$, temos que $x = \frac{a_1}{s_1}, y = \frac{a_2}{s_2}$, com $a_1, a_2 \in A$ e $s_1, s_2 \in S$. Assim, $xy = \frac{a_1 a_2}{s_1 s_2} = \frac{a_1 a_2}{s_1 s_2} = \frac{a_2 a_1}{s_2 s_1} = \frac{a_2 a_1}{s_2 s_1} = yx$. $\blacksquare$
2. $A \subset S^{-1}A$. De fato, basta considerarmos a aplicação $i : A \rightarrow S^{-1}A$, que a cada $x \in A$, $i(x) = \frac{x}{1}$. $\blacksquare$
3. Se $S = A - (0)$, então $S^{-1}A = K$. De fato, temos que $K = \left\{ \frac{a}{b}; a, b \in A \text{ e } b \neq 0 \right\} = \left\{ \frac{a}{b}; a \in A \text{ e } b \in A - (0) \right\} = \left\{ \frac{a}{b}; a \in A \text{ e } b \in S \right\} = S^{-1}A$. $\blacksquare$
4. Se $S = \{1\}$ ou $S = A^*$, então $S^{-1}A = A$. De fato, temos:
 - (i) Se $S = \{1\}$, temos $S^{-1}A = \left\{ \frac{a}{s}; a \in A \text{ e } s \in S = \{1\} \right\} = \left\{ \frac{a}{1}; a \in A \right\} = A$.
 - (ii) Se $S = A^*$, temos pela propriedade (2) que $A \subset S^{-1}A$. Por outro lado, temos que $S^{-1}A = \left\{ \frac{a}{s}; a \in A \text{ e } s \in S = A^* \right\} = \{as^{-1}; a \in A \text{ e } s^{-1} \in A^*\} \subset A$. Portanto, $S^{-1}A = A$. $\blacksquare$

Proposição 2.9.1 *Sejam A um domínio, S um subconjunto de $A - (0)$, fechado sob a multiplicação com $1 \in S$ e $S^{-1}A = \mathfrak{A}$. Para todo ideal $\mathfrak{b}$ de $\mathfrak{A}$, temos que $(\mathfrak{b} \cap A)\mathfrak{A} = \mathfrak{b}$, e assim a aplicação que a cada $\mathfrak{b}$ associa $\mathfrak{b} \cap A$ é uma injeção crescente do conjunto dos ideais de $\mathfrak{A}$ no conjunto dos ideais de A , com relação a inclusão.*

Demonstração: Mostraremos primeiramente que $(\mathfrak{b} \cap A)\mathfrak{A} = \mathfrak{b}$. Como $\mathfrak{b} \cap A \subset \mathfrak{b}$, segue que $(\mathfrak{b} \cap A)\mathfrak{A} \subset \mathfrak{b}\mathfrak{A} \stackrel{\mathfrak{b} \subset \mathfrak{A}}{=} \mathfrak{b}$. Por outro lado, se $x \in \mathfrak{b}$, temos que $x = \frac{a}{s}$, com $a \in A$ e $s \in S$. Como $\mathfrak{b}$ é um ideal de $\mathfrak{A}$ e $A \subset \mathfrak{A}$, segue que $sa \in \mathfrak{b}$. Portanto, $a \in \mathfrak{b}$ e $a \in A$, ou seja, $a \in \mathfrak{b} \cap A$. Assim, $x = \frac{1}{s}a \in (\mathfrak{b} \cap A)\mathfrak{A}$, ou seja, $\mathfrak{b} \subset (\mathfrak{b} \cap A)\mathfrak{A}$. Portanto, $(\mathfrak{b} \cap A)\mathfrak{A} = \mathfrak{b}$. Para provarmos a segunda parte consideraremos os seguintes conjuntos $\mathcal{W} = \{\text{conjuntos dos ideais de } \mathfrak{A}\}$ e $\mathcal{Y} = \{\text{conjuntos dos ideais de } A\}$, e mostraremos, que a aplicação $\varphi : \mathcal{W} \rightarrow \mathcal{Y}$ é uma injeção crescente. Temos que $\mathfrak{b} \cap A$ é um ideal de A , pois

- $0 \in \mathfrak{b} \cap A$, pois $0 \in \mathfrak{b}$ e $0 \in A$.
- $\forall a, b \in \mathfrak{b} \cap A$, temos $(a \in \mathfrak{b} \text{ e } a \in A) \text{ e } (b \in \mathfrak{b} \text{ e } b \in A) \implies a + b \in \mathfrak{b} \text{ e } a + b \in A \implies a + b \in \mathfrak{b} \cap A$.
- $\forall a \in A \text{ e } b \in \mathfrak{b} \cap A$, temos $a \in A, b \in \mathfrak{b} \text{ e } b \in A$, mas $a \in A \subset \mathfrak{A}$, então $a \in \mathfrak{A}$, daí $ab \in \mathfrak{b}$ e $ab \in A$, assim $ab \in \mathfrak{b} \cap A$.

Assim, se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais de $\mathfrak{A}$, tais que $\mathfrak{a} = \mathfrak{b} \implies \mathfrak{a} \cap A = \mathfrak{b} \cap A \implies \varphi(\mathfrak{a}) = \varphi(\mathfrak{b})$, ou seja, φ está bem definida. Agora mostraremos que φ é injetora e crescente. Sejam $\mathfrak{a}, \mathfrak{b}$ ideais de $\mathfrak{A}$, tais que $\varphi(\mathfrak{a}) = \varphi(\mathfrak{b}) \implies \mathfrak{a} \cap A = \mathfrak{b} \cap A \implies (\mathfrak{a} \cap A)\mathfrak{A} = (\mathfrak{b} \cap A)\mathfrak{A} \implies \mathfrak{a} = \mathfrak{b}$, ou seja, φ é injetiva. Agora se $\mathfrak{a} \subset \mathfrak{b} \implies \mathfrak{a} \cap A \subset \mathfrak{b} \cap A \implies \varphi(\mathfrak{a}) \subset \varphi(\mathfrak{b})$, ou seja, φ é crescente. $\blacksquare$

Corolário 2.9.1 *Se A é um domínio Noetheriano, então todo anel de frações $\mathfrak{A} = S^{-1}A$ é um anel Noetheriano.*

Demonstração: Pela Proposição 2.9.1 temos que $\varphi : \mathcal{W} \rightarrow \mathcal{V}$ é uma aplicação injetiva crescente. Se $\mathfrak{b}_1, \mathfrak{b}_2, \dots, \mathfrak{b}_n, \dots$ é uma seqüência de ideais de A , tais que $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \dots \subset \mathfrak{b}_n \subset \dots$, e como φ é crescente, temos que $\varphi(\mathfrak{b}_1) \subset \varphi(\mathfrak{b}_2) \subset \dots \subset \varphi(\mathfrak{b}_n) \subset \dots$. Do fato de que $\varphi(\mathfrak{b}_i)$ é um ideal de A , para todo i , e A ser Noetheriano, segue que $\exists n_0 \in \mathbb{N}$, tal que $\varphi(\mathfrak{b}_{n_0}) = \varphi(\mathfrak{b}_n)$, $\forall n \geq n_0$, e como φ é injetora, temos que $\mathfrak{b}_{n_0} = \mathfrak{b}_n, \forall n \geq n_0$, ou seja, $(\mathfrak{b}_n)$ é uma seqüência estacionária de $\mathfrak{A}$. Portanto, $\mathfrak{A}$ é Noetheriano. $\blacksquare$

Proposição 2.9.2 *Sejam A um domínio e S um subconjunto de $A - (0)$, fechado sob a multiplicação com $1 \in S$ e denotemos $S^{-1}A = \mathfrak{A}$. A aplicação que a cada $\mathfrak{q}$ associa $\mathfrak{q} \cap A$ é um isomorfismo do conjunto parcialmente ordenado dos ideais primos de $\mathfrak{A}$ no conjunto parcialmente ordenado dos ideais primos $\mathfrak{p}$ que satisfazem $\mathfrak{p} \cap S = \emptyset$, e sua inversa é a aplicação que a cada $\mathfrak{p}$ associa $\mathfrak{p}\mathfrak{A}$.*

Demonstração: Dados os conjuntos, $\mathcal{U} = \{\text{conjunto dos ideais primos } \mathfrak{q} \text{ de } \mathfrak{A}\}$ e $\mathcal{V} = \{\text{conjunto dos ideais primos } \mathfrak{p} \text{ de } A, \text{ tal que } \mathfrak{p} \cap S = \emptyset\}$, consideremos as aplicações,

$$\begin{array}{ccc} \varphi : \mathcal{U} \longrightarrow \mathcal{V} & & \psi : \mathcal{V} \longrightarrow \mathcal{U} \\ \mathfrak{q} \longmapsto \mathfrak{q} \cap A & \text{e} & \mathfrak{p} \longmapsto \mathfrak{p}\mathfrak{A} \end{array}$$

Pela Proposição 2.9.1 temos que φ é uma aplicação injetora crescente e pela Proposição 2.6.3 temos que se $\mathfrak{q}$ é um ideal primo de $\mathfrak{A}$, então $\mathfrak{q} \cap A$ é um ideal primo de A . Se $\mathfrak{p} = \mathfrak{q} \cap A$, é um ideal primo de A , mostraremos que $\mathfrak{p} \cap S = \emptyset$. Suponhamos que $\mathfrak{p} \cap S \neq \emptyset$, ou seja, existe um $x \in \mathfrak{p} \cap S$. Então, $x \in \mathfrak{p}$ e $x \in S$. Por outro lado, como $\varphi(\mathfrak{q}) = \mathfrak{q} \cap A = \mathfrak{p} \subset \mathfrak{q}$, segue que $x \in \mathfrak{q}$ e $x \in S$. Mas $1 = \frac{1}{x}x \in \mathfrak{A}\mathfrak{q}$, o que é um absurdo, pois $\mathfrak{q}$ é um ideal primo. Portanto, $\mathfrak{p} \cap S = \emptyset$, ou seja, φ está bem definida. Agora vamos mostrar que ψ está bem definida. Seja $\mathfrak{p} \in \mathcal{V}$. Temos que mostrar $\mathfrak{p}\mathfrak{A}$ é um ideal primo de $\mathfrak{A}$ e que $\mathfrak{p}\mathfrak{A} \cap A = \mathfrak{p}$. Assim, se $x \in \mathfrak{p}\mathfrak{A}$ temos

$x = \sum_{i=1}^n \frac{a_i}{s_i} p_i$, com $a_i \in A$, $s_i \in S$ e $p_i \in \mathfrak{p}$, para todo $i = 1, \dots, n$. Tomando $s = s_1 \dots s_n$ e $\frac{b_i}{s} = \frac{a_i}{s_i}$, $i = 1, \dots, n$, obtemos que $x = \sum_{i=1}^n \frac{b_i}{s} p_i = \frac{1}{s} \sum_{i=1}^n b_i p_i$ e como $\sum_{i=1}^n b_i p_i \in \mathfrak{p}$, segue que $x = \frac{p}{s}$ com $p \in \mathfrak{p}$ e $s \in S$. Como $\mathfrak{p} \cap S = \emptyset$, segue que $1 \notin \mathfrak{p}\mathfrak{A}$, ou seja, 1 não pode ser escrito na forma $\frac{1}{s}$ com $p \in \mathfrak{p}$ e $s \in S$. Agora, sejam $x = \frac{a}{s} \in \mathfrak{A}$ e $y = \frac{b}{t} \in \mathfrak{U}$, tal que $xy \in \mathfrak{p}\mathfrak{A}$. Então, $xy = \frac{ab}{st} = \frac{p}{u}$ com $p \in \mathfrak{p}$ e $u \in S$, ou seja, $abu = pst \in \mathfrak{p}$. Como $\mathfrak{p} \cap S = \emptyset$, temos que $u \notin \mathfrak{p}$, e como $\mathfrak{p}$ é primo, segue que $ab \in \mathfrak{p}$, e assim $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Assim, $x = \frac{a}{s} \in \mathfrak{p}\mathfrak{A}$ ou $y = \frac{b}{t} \in \mathfrak{p}\mathfrak{A}$, ou seja, $\mathfrak{p}\mathfrak{A}$ é um ideal primo. Mostremos agora que $\mathfrak{p}\mathfrak{A} \cap A = \mathfrak{p}$. Como $\mathfrak{p} \subset A$ e $\mathfrak{p} \subset \mathfrak{p}\mathfrak{A}$, então $\mathfrak{p} \subset \mathfrak{p}\mathfrak{A} \cap A$. Por outro lado, seja $x \in \mathfrak{p}\mathfrak{A} \cap A$. Então, $x = \frac{p}{s}$, com $p \in \mathfrak{p}$ e $s \in S$ e daí $xs \in \mathfrak{p}$. Como $\mathfrak{p}$ é um ideal primo e $s \notin \mathfrak{p}$, segue que $x \in \mathfrak{p}$, ou seja, $\mathfrak{p}\mathfrak{A} \cap A \subset \mathfrak{p}$. Portanto, $\mathfrak{p}\mathfrak{A} \cap A = \mathfrak{p}$. Finalmente, temos que $(\varphi \circ \psi)(\mathfrak{p}) = \varphi(\psi(\mathfrak{p})) = \varphi(\mathfrak{p}\mathfrak{A}) = \mathfrak{p}\mathfrak{A} \cap A = \mathfrak{p}$ e $(\psi \circ \varphi)(\mathfrak{q}) = \psi(\varphi(\mathfrak{q})) = \psi(\mathfrak{q} \cap A) = (\mathfrak{q} \cap A)\mathfrak{A} = \mathfrak{q}$, ou seja, $\varphi = \psi^{-1}$. Assim, φ é um isomorfismo. ■

Teorema 2.9.1 *Sejam A um domínio, B um subanel de A , S um subconjunto de B fechado sob a multiplicação com $1 \in S$ e $0 \notin S$ e F o anel dos inteiros de A sobre B . Então, o anel dos inteiros de $\mathfrak{A} = S^{-1}A$ sobre $\mathfrak{B} = S^{-1}B$ é $\mathfrak{F} = S^{-1}F$.*

Demonstração: A prova deste teorema consiste em mostrar que todo elemento de $\mathfrak{A}$ que é inteiro sobre $\mathfrak{B}$ pertence a $\mathfrak{F}$ e que todo elemento de $\mathfrak{F}$ é inteiro sobre $\mathfrak{B}$.

1) Seja $x \in \mathfrak{A}$ um elemento inteiro sobre $\mathfrak{B}$. Assim, $x = \frac{a}{s}$ com $a \in A$ e $s \in S$ e existem $\frac{a_i}{t_i}$, $i = 1, \dots, n$ com $a_i \in \mathcal{O}_L$ e $t_i \in S$, tal que $x^n + \frac{a_{n-1}}{t_{n-1}}x^{n-1} + \dots + \frac{a_0}{t_0} = 0$, ou seja, $\left(\frac{a}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{a}{s}\right)^{n-1} + \dots + \frac{a_0}{t_0} = 0$. Multiplicando ambos os lados desta igualdade por $(t_0 \dots t_{n-1})^n$, temos $(t_0 \dots t_{n-1}a)^n + a_{n-1}s(t_0t_1 \dots t_{n-2})(t_0t_1 \dots t_{n-1}a)^{n-1} + \dots + a_0(t_1 \dots t_{n-1}s) = 0$, o que implica que $t_0 \dots t_{n-1}a \in F$, ou seja, é um inteiro de A sobre B . Assim, existe $f \in F$, tal que $t_0 \dots t_{n-1}a = f$, e portanto, $a = \frac{f}{t_0 \dots t_{n-1}} \in \mathfrak{F}$. Como $x = \frac{a}{s}$, temos que $x = \frac{f}{t_0 \dots t_{n-1}s} \in \mathfrak{F}$.

2) Se $x \in \mathfrak{F}$, então $x = \frac{f}{s}$, com $f \in F$ e $s \in S$. Como f é inteiro de A sobre B , f satisfaz uma equação do tipo $(f)^n + b_{n-1}(f)^{n-1} + \dots + b_0 = 0$, com $b_i \in B$, $i = 0, \dots, n-1$. Multiplicando ambos os lados desta igualdade por $\left(\frac{1}{s}\right)^n$, obtemos $\left(\frac{f}{s}\right)^n + \frac{b_{n-1}}{s}\left(\frac{f}{s}\right)^{n-1} + \dots + \frac{b_0}{s^n} = 0$,

ou seja, $x^n + \frac{b_{n-1}}{s}x^{n-1} + \dots + \frac{b_0}{s^n} = 0$. Como $\frac{b_i}{s^j} \in \mathfrak{B}$, para todo $i = 0, \dots, n-1$ e $j = 1, \dots, n$, segue que x é inteiro sobre $\mathfrak{B}$. $\blacksquare$

Corolário 2.9.2 *Se A é um anel integralmente fechado, então todo anel de frações $S^{-1}A$ é integralmente fechado.*

Demonstração: Seja K o corpo de frações do anel A e seja B o anel dos inteiros de K sobre A . Por hipótese, como A é integralmente fechado, temos que $A = B$, e assim pelo Teorema 2.9.1 decorre que $S^{-1}A = S^{-1}B$. $\blacksquare$

Teorema 2.9.2 *Se A é um anel de Dedekind, então todo anel de frações $S^{-1}A = \mathfrak{A}$ é um anel de Dedekind.*

Demonstração: Como por hipótese A é um anel de Dedekind, segue que A é integralmente fechado. Pelos Corolários 2.9.1 e 2.9.2 temos que $\mathfrak{A}$ é Noetheriano e integralmente fechado. Agora resta mostrarmos que todo ideal primo não nulo de $\mathfrak{A}$ é maximal. Seja $\mathfrak{q}$ um ideal primo não nulo de $\mathfrak{A}$. Considerando o isomorfismo φ dado pela Proposição 2.9.2, temos que $\varphi(\mathfrak{q}) = \mathfrak{q} \cap A = \mathfrak{p}$ é um ideal primo de A , e portanto, é um ideal maximal, pois A é Dedekind. Se $\mathfrak{q}$ não for maximal, então existe um ideal J de $\mathfrak{A}$, tal que $\mathfrak{q} \subsetneq J \subsetneq \mathfrak{A}$. Pelo isomorfismo φ , temos $\varphi(\mathfrak{q}) = \mathfrak{p} \subsetneq \varphi(J) \subsetneq A$, o que é um absurdo, pois $\mathfrak{p}$ é maximal. Portanto, o ideal $\mathfrak{q}$ é maximal. $\blacksquare$

Teorema 2.9.3 *Sejam A um anel de Dedekind, $\mathfrak{p}$ um ideal não nulo de A e $S = A - \mathfrak{p}$. Então, $S^{-1}A = \mathfrak{A}$ é um anel principal, mas precisamente existe um elemento primo $p \in \mathfrak{A}$, tal que os ideais não nulos de $\mathfrak{A}$ são da forma $\langle p^n \rangle$, com $n \geq 0$.*

Demonstração: Temos que $\mathfrak{p}$ é o único ideal primo não nulo de A , tal que $\mathfrak{p} \cap S = \emptyset$, pois se existisse um outro ideal $\mathfrak{p}_1$ de A , tal que $\mathfrak{p}_1 \cap S = \emptyset$, teríamos que $\mathfrak{p}_1 \subset \mathfrak{p}$. Logo, $\mathfrak{p}_1 = \mathfrak{p}$ uma vez que $\mathfrak{p}$ e $\mathfrak{p}_1$ são maximais. Pela Proposição 2.9.2, temos que o único ideal primo não nulo de $\mathfrak{A}$ é $\mathfrak{b} = \mathfrak{p}\mathfrak{A}$, e pelo Teorema 2.9.2, temos que $\mathfrak{A}$ é um anel de Dedekind. Assim, pelo Teorema 2.7.3 os ideais não nulos de $\mathfrak{A}$ são da forma $\mathfrak{b}^n, n \geq 0$. Agora, considerando $p \in \mathfrak{b} \setminus \mathfrak{b}^2$ temos que $\langle p \rangle \subset \mathfrak{b}$, mas $\langle p \rangle \not\subset \mathfrak{b}^2$. Logo, $\langle p \rangle = \mathfrak{b}$ e daí segue que $\langle p^n \rangle = \mathfrak{b}^n; n \geq 0$. Portanto, $\mathfrak{A}$ é principal e todos os seus ideais são da forma $\langle p^n \rangle; n \geq 0$. Além disso, p é um elemento primo pois, $\langle p \rangle = \mathfrak{b}$ é maximal, e então p é irredutível e como $\mathfrak{A}$ é principal, segue que p é primo. $\blacksquare$

Teorema 2.9.4 *Sejam A um domínio, S um subconjunto de $A - (0)$ fechado sob a multiplicação com $1 \in S$ e $\mathfrak{m}$ um ideal maximal de A disjuncto de S . Então, $\mathfrak{A}/\mathfrak{m}\mathfrak{A} \simeq A/\mathfrak{m}$.*

Demonstração: Sendo $\mathfrak{m}$ um ideal maximal de A , segue que $\mathfrak{m}$ também é um ideal primo de A , então pela Proposição 2.9.2, $\mathfrak{m}\mathfrak{A}$ é um ideal primo em $\mathfrak{A}$. Consideremos a composição de homomorfismos $A \xrightarrow{i} \mathfrak{A} \xrightarrow{\varphi} \mathfrak{A}/\mathfrak{m}\mathfrak{A}$, onde i é a inclusão e φ a projeção e $\Phi = \varphi \circ i : A \rightarrow \mathfrak{A}/\mathfrak{m}\mathfrak{A}$. Temos que φ é um homomorfismo e $\text{Ker}(\Phi) = \mathfrak{m}\mathfrak{A} \cap A = \mathfrak{m}$. De fato, $x \in \text{Ker}(\Phi) \Rightarrow \Phi(x) = \bar{0}$ e $x \in A \Rightarrow x + \mathfrak{m}\mathfrak{A} = \bar{0}$ e $x \in A \Rightarrow x \in \mathfrak{m}\mathfrak{A}$ e $x \in A \Rightarrow x \in \mathfrak{m}\mathfrak{A} \cap A$, ou seja, $\text{Ker}(\Phi) \subset \mathfrak{m}\mathfrak{A} \cap A$. Por outro lado, $y \in \mathfrak{m}\mathfrak{A} \cap A \Rightarrow y \in \mathfrak{m}\mathfrak{A}$ e $y \in A \Rightarrow \Phi(y) = \bar{0} \Rightarrow y \in \text{Ker}(\Phi)$, assim $\mathfrak{m}\mathfrak{A} \cap A \subset \text{Ker}(\Phi)$. Portanto, $\text{Ker}(\Phi) = \mathfrak{m}\mathfrak{A} \cap A = \mathfrak{m}$. Agora, vamos mostrar que φ é sobrejetora. Seja $x \in \mathfrak{A}$, assim $x = \frac{a}{s}$ com $a \in A, s \in S$ e seja $\bar{x} = x + \mathfrak{m}\mathfrak{A}$. Como $S \cap \mathfrak{m} = \emptyset$, temos que $s \notin \mathfrak{m}$, ou seja, $\bar{s} \neq \bar{0}$ e como $A/\mathfrak{m}$ é corpo, segue que $\bar{s}$ é invertível módulo $\mathfrak{m}$. Assim, existe $\bar{r} = r + \mathfrak{m} \in A/\mathfrak{m}$, $r \in A$, tal que $\bar{s} \bar{r} \equiv \bar{1} \pmod{\mathfrak{m}}$, ou seja, $rs - 1 \in \mathfrak{m}$. Logo, $ra - x = ra - \frac{a}{s} \in \mathfrak{m} = (rs - 1)\frac{a}{s} \in \mathfrak{m}\mathfrak{A}$, e portanto, $\varphi(ar) = ar + \mathfrak{m}\mathfrak{A} = x + \mathfrak{m}\mathfrak{A}$, ou seja, φ é sobrejetora. Portanto, pelo Teorema 1.1.1, segue que $\mathfrak{A}/\mathfrak{m}\mathfrak{A} \simeq A/\mathfrak{m}$. $\blacksquare$

Sejam A um anel de Dedekind de característica zero, K seu corpo de frações, L uma extensão finita de K de grau n e B o anel dos inteiros de L sobre A . Seja $\mathfrak{p}$ um ideal primo não nulo de A . Então, $B\mathfrak{p}$ é um ideal de B e pelo Teorema 2.7.3 é expresso de modo único como $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}'_i e'_i$, com os $\mathfrak{b}'_i$ s ideais primos distintos de B e os e'_i s inteiros positivos. Além disso, como A é Dedekind, temos pelo Teorema 2.7.1 que B é um anel de Dedekind e um A -módulo finitamente gerado.

Lema 2.9.1 *Se $\mathfrak{b}$ é um ideal primo de B , então $\mathfrak{b} \cap A = \mathfrak{p}$ se, e somente se, $\mathfrak{b} \supset B\mathfrak{p}$.*

Demonstração: Por hipótese temos, $\mathfrak{b} \cap A = \mathfrak{p} \Rightarrow \mathfrak{p} \subset \mathfrak{b} \Rightarrow \mathfrak{p}B \subset \mathfrak{b}B = \mathfrak{b} \Rightarrow \mathfrak{b} \supset \mathfrak{p}B$. Por outro lado, seja $\mathfrak{b} \subset B$ um ideal primo, tal que $\mathfrak{b} \supset \mathfrak{p}B$. Pela Proposição 2.6.3, temos que $\mathfrak{p} \cap A$ é um ideal primo de A e que $\mathfrak{b} \cap A \neq A$, uma vez que $1 \notin \mathfrak{b}$. Como $\mathfrak{p} \subset \mathfrak{b}$ e $\mathfrak{p} \subset A$, temos $\mathfrak{p} \subset \mathfrak{b} \cap A$, mas $\mathfrak{p}$ é maximal, assim $\mathfrak{p} = \mathfrak{b} \cap A$. $\blacksquare$

Lema 2.9.2 $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i} \iff B\mathfrak{p} \subset \mathfrak{b}_i, \forall i = 1, \dots, q.$

Demonstração: Se $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i}$, temos que $B\mathfrak{p} \subset \mathfrak{b}_i$, para todo $i = 1, \dots, q$. Por outro lado, suponhamos que $B\mathfrak{p} \subset \mathfrak{b}_i$, para todo $i = 1, \dots, q$, e que $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{q}_i^{e_i}$, com q_i ideais

primos de B . Como $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{q}_i^{e_i} \subset \mathfrak{b}_i$, para $i = 1, \dots, q$, pela Proposição 2.6.4, segue que $\mathfrak{q}_{i_0} \subset \mathfrak{b}_i$, para algum i_0 . Como $\mathfrak{q}_{i_0}$ é maximal, segue que $\mathfrak{q}_{i_0} = \mathfrak{b}_i$. Continuando desta maneira mostramos que $\mathfrak{q}_i = \mathfrak{b}_i$, para todo i , ou seja, $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i}$. $\blacksquare$

Observações 2.9.1 1) Temos que $A/\mathfrak{p}$ pode ser identificado como um subcorpo de $B/\mathfrak{b}_i$, $\forall i = 1, \dots, q$. **De fato:** Sejam os seguintes homomorfismos $A \xrightarrow{i} B \xrightarrow{\varphi} B/\mathfrak{b}_i$, onde i é a inclusão e φ é a projeção. Assim, $\varphi \circ i = \psi$ é um homomorfismo com $\text{Ker} \psi = \mathfrak{b}_i \cap A = \mathfrak{p}$. Temos pelo Teorema 1.1.1 $A/\mathfrak{p} \simeq \text{Im}(\psi)$, ou seja, $A/\mathfrak{p}$ é visto como um subcorpo de $B/\mathfrak{b}_i$, $i = 1, \dots, q$. $\blacksquare$

2) Como $A/\mathfrak{p}$ e $B/\mathfrak{b}_i$ são corpos e B é um A -módulo finitamente gerado, segue que $B/\mathfrak{b}_i$ é um espaço vetorial de dimensão finita sobre $A/\mathfrak{p}$. **De fato:** Com as seguintes operações,

$$+ : B/\mathfrak{b}_i \times B/\mathfrak{b}_i \longrightarrow B/\mathfrak{b}_i$$

$$(\bar{x}, \bar{y}) \longmapsto \bar{x} + \bar{y}$$

$$\bullet : A/\mathfrak{p} \times B/\mathfrak{b}_i \longrightarrow B/\mathfrak{b}_i$$

$$(\bar{a}, \bar{x}) \longmapsto \bar{a} \bar{x}$$

temos que $B/\mathfrak{b}_i$ é um espaço vetorial sobre $A/\mathfrak{p}$, e $B/\mathfrak{b}_i$ tem dimensão finita, pois sendo $\{x_1, \dots, x_n\}$ os geradores de B , temos que se $b \in B$, então $b = a_1 x_1 + \dots + a_n x_n$, com $a_i \in A$. Assim, $\bar{b} = \bar{a}_1 \bar{x}_1 + \dots + \bar{a}_n \bar{x}_n$, com $\bar{a}_i = a_i + \mathfrak{p}$. Portanto, $\{\bar{x}_1, \dots, \bar{x}_n\}$ gera como um espaço vetorial $B/\mathfrak{b}_i$ sobre $A/\mathfrak{p}$. $\blacksquare$

3) $B\mathfrak{p} \cap A = \mathfrak{p}$. **De fato:** Temos que $\mathfrak{p} \subset B\mathfrak{p}$ e $\mathfrak{p} \subset A$, ou seja, $\mathfrak{p} \subset B\mathfrak{p} \cap A$. Por outro lado, temos que $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i} \subset \mathfrak{b}_i, \forall i = 1, \dots, q$. Portanto, $B\mathfrak{p} \cap A \subset \mathfrak{b}_i \cap A = \mathfrak{p}$. Assim, $B\mathfrak{p} \cap A = \mathfrak{p}$. $\blacksquare$

4) $B/B\mathfrak{p}$ é um espaço vetorial sobre $A/\mathfrak{p}$ de dimensão finita. **De fato:** Consideremos os seguintes homomorfismos $A \xrightarrow{i} B \xrightarrow{\varphi} B/B\mathfrak{p}$, onde i é a inclusão e φ é a projeção. Assim, $\varphi \circ i = \psi$ é um homomorfismo com $\text{Ker} \psi = B\mathfrak{p} \cap A = \mathfrak{p}$. Logo, pelo Teorema 1.1.1, temos que $A/\mathfrak{p} \simeq \text{Im}(\psi)$, ou seja, podemos ver $B/B\mathfrak{p}$ como um espaço vetorial sobre $A/\mathfrak{p}$. Agora, se $\{x_1, \dots, x_n\}$ são os geradores de B sobre A , então se $\bar{b} = b + B\mathfrak{p}$, com $b = a_1 x_1 + \dots + a_n x_n$, $a_i \in A$, $i = 1, \dots, n$. Portanto, $\bar{b} = \bar{a}_1 \bar{x}_1 + \dots + \bar{a}_n \bar{x}_n$, ou seja, $\{\bar{x}_1, \dots, \bar{x}_n\}$ é um conjunto de geradores de $B/B\mathfrak{p}$ como um espaço vetorial sobre $A/\mathfrak{p}$, ou seja, a dimensão é finita. $\blacksquare$

Definição 2.9.2 O grau f_i da extensão $B/\mathfrak{b}_i$ sobre $A/\mathfrak{p}$ é chamado de **grau residual** (ou grau de inércia) de $\mathfrak{b}_i$ sobre A , e o expoente e_i é chamado de **índice de ramificação** de $\mathfrak{b}_i$ sobre A .

Teorema 2.9.5 (Igualdade Fundamental) Sejam A um anel de Dedekind de característica zero, K seu corpo de frações, L uma extensão finita de K de grau n , B o anel dos inteiros de L sobre A , $\mathfrak{p}$ um ideal primo não nulo de A e $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i}$, com os $\mathfrak{b}_i$'s ideais primos distintos de B e os e_i 's inteiros positivos. Então, $\sum_{i=1}^q e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n$.

Demonstração: Consideremos a seqüência de ideais $B \supset \mathfrak{b}_1 \supset \mathfrak{b}_1^2 \supset \dots \supset \mathfrak{b}_1^{e_1} \supset \mathfrak{b}_1^{e_1} \mathfrak{b}_2 \supset \dots \supset \mathfrak{b}_1^{e_1} \mathfrak{b}_2^{e_2} \supset \dots \supset \mathfrak{b}_1^{e_1} \dots \mathfrak{b}_q^{e_q} = B\mathfrak{p}$. Dois elementos desta seqüência tem a forma $\mathfrak{b}$ e $\mathfrak{b}\mathfrak{b}_i$, sendo $\mathfrak{b}$ um produto de ideais. Afirmamos que não existe nenhum ideal estritamente contido entre $\mathfrak{b}$ e $\mathfrak{b}\mathfrak{b}_i$, pois se existisse um ideal $\mathfrak{q}$, tal que $\mathfrak{b} \supset \mathfrak{q} \supset \mathfrak{b}\mathfrak{b}_i \Rightarrow \mathfrak{b}^{-1}\mathfrak{b} \supset \mathfrak{b}^{-1}\mathfrak{q} \supset \mathfrak{b}^{-1}\mathfrak{b}\mathfrak{b}_i \Rightarrow B \supset \mathfrak{b}^{-1}\mathfrak{q} \supset B\mathfrak{b}_i = \mathfrak{b}_i \Rightarrow B \supset \mathfrak{b}^{-1}\mathfrak{q} \supset \mathfrak{b}_i \xRightarrow{\mathfrak{b}_i \text{ é maximal em } B} \mathfrak{b}^{-1}\mathfrak{q} = B$ ou $\mathfrak{b}^{-1}\mathfrak{q} = \mathfrak{b}_i \Rightarrow \mathfrak{q} = \mathfrak{b}B = \mathfrak{b}$ ou $\mathfrak{q} = \mathfrak{b}\mathfrak{b}_i$. Assim, não existe tal ideal $\mathfrak{q}$. Com as operações vista na Observação 2.9.1, temos que $\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i$ é um espaço vetorial sobre $B/\mathfrak{b}_i$, e assim seus subespaços são da forma $\mathfrak{q}/\mathfrak{b}\mathfrak{b}_i$ com $\mathfrak{b} \supset \mathfrak{q} \supset \mathfrak{b}\mathfrak{b}_i$. Mas como $\mathfrak{q} = \mathfrak{b}$ ou $\mathfrak{q} = \mathfrak{b}\mathfrak{b}_i$, segue que os únicos subespaços de $\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i$ são os triviais $\{0\}$ e $\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i$. Desta forma, $\dim_{\mathfrak{b}/\mathfrak{b}_i} \mathfrak{b}/\mathfrak{b}\mathfrak{b}_i = 1$, e então $|B/\mathfrak{b}_i| = |\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i|$ e $[\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i : B/\mathfrak{p}] = f_i$, pois $[B/\mathfrak{b}_i : A/\mathfrak{p}] = f_i$ e $[\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i : B/\mathfrak{b}_i] = 1$. Dado um índice i , podemos observar que existem exatamente e_i elementos consecutivos na seqüência dos ideais com o quociente da forma $\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i$, ou seja, de dimensão f_i sobre $A/\mathfrak{p}$. A dimensão total de $[B/B\mathfrak{p} : A/\mathfrak{p}]$ é igual a soma das dimensões dos quocientes que por sua vez é $[B/B\mathfrak{p} : A/\mathfrak{p}] = e_1 f_1 + e_2 f_2 + \dots + e_q f_q = \sum_{i=1}^q e_i f_i$. Agora, se A for principal a segunda igualdade é verdadeira. De fato, se A é principal temos que B é um A -módulo livre de posto n . Se $\{\alpha_1, \dots, \alpha_n\}$ é uma A -base de B , mostremos que $\{\alpha_1 + B\mathfrak{p}, \dots, \alpha_n + B\mathfrak{p}\}$ é uma base de $B/B\mathfrak{p}$ sobre $A/\mathfrak{p}$:

- $\forall \bar{\mathfrak{b}} \in B/B\mathfrak{p}$ temos $\bar{\mathfrak{b}} = \mathfrak{b} + B\mathfrak{p} \Rightarrow \bar{\mathfrak{b}} = (a_1\alpha_1 + \dots + a_n\alpha_n) + B\mathfrak{p} = (a_1\alpha_1 + B\mathfrak{p}) + \dots + (a_n\alpha_n + B\mathfrak{p}) = \overline{a_1\alpha_1} + \dots + \overline{a_n\alpha_n} = \overline{a_1} \overline{\alpha_1} + \dots + \overline{a_n} \overline{\alpha_n}$, com $\overline{a_i} \in A/\mathfrak{p}$, ou seja, gera.
- Mostremos que $\{\overline{\alpha_1}, \dots, \overline{\alpha_n}\}$ é linearmente independente. Se $\overline{a_1} \overline{\alpha_1} + \dots + \overline{a_n} \overline{\alpha_n} = \overline{0}$

em $B/B\mathfrak{p} \Rightarrow a_1\alpha_1 + \dots + a_n\alpha_n = \sum_{j=1}^s b_j p_j$; $b_j \in B$ e $p_i \in \mathfrak{p}$, $i = 1, \dots, s$. Mas para todo

j , $b_j \in B$ é gerado por $\{\alpha_1, \dots, \alpha_n\}$, ou seja, $\forall j$, $b_j = \sum_{i=1}^n c_{ji}\alpha_i$, com $c_{ij} \in A$. Então,

$$\sum_{i=1}^n a_i \alpha_i = \sum_{j=1}^s \left(\sum_{i=1}^n c_{ij} \alpha_i \right) p_j = \sum_{i=1}^n \left(\sum_{j=1}^s c_{ij} p_j \right) \alpha_i. \text{ Como } \{\alpha_1, \dots, \alpha_n\} \text{ é linearmente}$$

independente, segue que $a_i = \sum_{j=1}^s c_{ij} p_j \in \mathfrak{p}$, ou seja, $\bar{a}_i = \bar{0}$, $\forall i = 1, \dots, n$.

A demonstração no caso geral será feita por redução ao caso anterior. Temos por hipótese que A é um domínio de Dedekind. Assim, se $\mathfrak{p}$ é um ideal primo não nulo de A e se $S = A - \mathfrak{p}$, temos pelo Teorema 2.9.3 que $S^{-1}A$ é um anel principal e pelo Teorema 2.9.1 temos ainda que $S^{-1}B$ é o anel dos inteiros de $\mathbb{L}$ sobre $S^{-1}A$ e é um $S^{-1}A$ -módulo livre. Daí pelo caso anterior temos que $\left[\frac{S^{-1}B}{\mathfrak{p}S^{-1}B} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A} \right] = n$. Agora considerando a fatoração

do ideal $\mathfrak{p}S^{-1}B = \prod_{i=1}^q (S^{-1}\mathfrak{b}_i)^{e_i}$ no anel de Dedekind $S^{-1}B$, temos pela primeira parte da demonstração que $\left[\frac{S^{-1}B}{S^{-1}B\mathfrak{p}} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A} \right] = \sum e_i \left[\frac{S^{-1}B}{S^{-1}B\mathfrak{b}_i} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A} \right]$. Como $\frac{S^{-1}A}{\mathfrak{p}S^{-1}A} \simeq \frac{A}{\mathfrak{p}}$ e $\frac{S^{-1}B}{S^{-1}B\mathfrak{b}_i} \simeq \frac{B}{\mathfrak{b}_i}$, segue que $n = \left[\frac{S^{-1}B}{S^{-1}B\mathfrak{b}} : \frac{S^{-1}A}{\mathfrak{p}S^{-1}A} \right] = \sum_{i=1}^q e_i f_i$. $\blacksquare$

Sejam $K = \mathbb{Q}(\sqrt{d})$, d livre de quadrados, $\mathcal{O}_K$ o anel dos inteiros de K e $p \in \mathbb{Z}$ um número primo. Pelo Teorema 2.7.3, temos que $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{B}_i^{e_i}$, com $\mathfrak{B}_i$ ideais primos de $\mathcal{O}_K$, tal que $\mathfrak{B}_i \cap \mathcal{O}_K = \langle p \rangle$. Do Teorema 2.9.5, temos que $q \leq 2$, e assim temos os seguintes fatos:

- (1) $q = 2$, $e_1 = e_2 = 1$, e $f_1 = f_2 = 1$. Neste caso, dizemos que p **decompõe** em K .
- (2) $q = 1$, $e_1 = 1$ e $f_1 = 2$. Neste caso, dizemos que p **permanece** primo em K .
- (3) $q = 1$, $e_1 = 2$ e $f_1 = 1$. Neste caso, dizemos que p **ramifica** em K .

Corolário 2.9.3 *Sejam $K \subset \mathbb{L}$ corpos numéricos, tal que $n = [\mathbb{L} : K]$, $\mathcal{O}_K$ e $\mathcal{O}_L$ os anéis dos inteiros de K e $\mathbb{L}$, respectivamente. Se $\mathfrak{p}_n \subset \mathcal{O}_K$ é um ideal primo, então $\mathcal{N}(\mathfrak{p}\mathcal{O}_L) = \mathcal{N}_{\mathcal{O}_K}(\mathfrak{p})^n$.*

Demonstração: Temos que, $\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^n \mathfrak{b}_i^{e_i}$, com $\mathfrak{b}_i \cap \mathcal{O}_K = \mathfrak{p}$, $[\mathcal{O}_L/\mathfrak{b}_i : \mathcal{O}_K/\mathfrak{p}] = f_i$, para

$$i = 1, \dots, n \text{ e } \mathfrak{b}_i \text{ ideais primos de } \mathcal{O}_L. \text{ Assim, } \mathcal{N}_{\mathcal{O}_L}(\mathfrak{p}\mathcal{B}) = \mathcal{N}_{\mathcal{O}_L} \left(\prod_{i=1}^n \mathfrak{b}_i^{e_i} \right) = \prod_{i=1}^n (\mathcal{N}_{\mathcal{O}_L}(\mathfrak{b}_i))^{e_i} =$$

$$\prod_{i=1}^n (\mathcal{N}_{\mathcal{O}_K}(\mathfrak{p})^{f_i})^{e_i} = \mathcal{N}_{\mathcal{O}_K}(\mathfrak{p})^n. \quad \blacksquare$$

Proposição 2.9.3 Com as mesmas notações do Teorema 2.9.5 temos que o anel $B/B\mathfrak{p}$ é isomorfo ao anel $\prod_{i=1}^q B/\mathfrak{b}_i^{e_i}$.

Demonstração: Temos que $\mathfrak{b}_i$ é o único ideal maximal de B que contém $\mathfrak{b}_i^{e_i}$, pois se existir $\mathfrak{m}$ um ideal maximal de B , tal que $\mathfrak{m} \supset \mathfrak{b}_i^{e_i}$, temos pela Proposição 2.6.4 que $\mathfrak{m} \supset \mathfrak{b}_i$, para algum i . Como $\mathfrak{b}_i$ é maximal segue que $\mathfrak{m} = \mathfrak{b}_i$. Agora, temos que $\mathfrak{b}_i^{e_i} + \mathfrak{b}_j^{e_j} = B$, para $i \neq j$, uma vez se $\mathfrak{b}_i^{e_i} + \mathfrak{b}_j^{e_j} \subsetneq B$, então existe um ideal maximal $\mathfrak{m}$ de B , tal que $\mathfrak{b}_i^{e_i} + \mathfrak{b}_j^{e_j} \subset \mathfrak{m} \subset B$. Como $\mathfrak{b}_i^{e_i} \subset \mathfrak{b}_i^{e_i} + \mathfrak{b}_j^{e_j}$, segue que $\mathfrak{b}_i^{e_i} \subset \mathfrak{m}$, ou seja, $\mathfrak{b}_i \subset \mathfrak{m}$, e como $\mathfrak{b}_i$ é maximal, segue que $\mathfrak{b}_i = \mathfrak{m}$. De modo análogo, temos que $\mathfrak{b}_j = \mathfrak{m}$, o que é um absurdo. Portanto, $\mathfrak{b}_i^{e_i} + \mathfrak{b}_j^{e_j} = B$. Agora, o resultado segue pela Proposição 1.1.2. $\blacksquare$

Lema 2.9.3 (Kummer) Sejam K um corpo de números, $\mathcal{O}_K$ o seu anel dos inteiros algébricos e $\theta \in \mathcal{O}_K$, tal que $K = \mathbb{Q}(\theta)$. Dados um número primo p , tal que p não divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ e $f(x)$ o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem polinômios irredutíveis $p_1(X), \dots, p_q(X) \in \mathbb{Z}[X]$, $e_1, \dots, e_q \in \mathbb{N}^*$, tais que $f(X) \equiv p_1(X)^{e_1} \dots p_q(X)^{e_q} \pmod{p\mathbb{Z}[X]}$ e além disso,

1. $\mathfrak{p}_i = (p, p_i(\theta)) = p\mathcal{O}_K + p_i(\theta)\mathcal{O}_K$ são os ideais primos de $\mathcal{O}_K$ acima de $p\mathbb{Z}$, $i = 1, \dots, q$.

$$2. p\mathcal{O}_K = \prod_{i=1}^q \mathfrak{p}_i^{e_i}.$$

$$3. \left[\frac{\mathcal{O}_K}{\mathfrak{p}_i} : \frac{\mathbb{Z}}{p\mathbb{Z}} \right] = \partial p_i(X) = f_i.$$

2.10 Discriminante e ramificação

Sejam A um anel de Dedekind de característica zero, K seu corpo de frações, L uma extensão finita de K de grau n e B o anel dos inteiros de L sobre A . Sejam $\mathfrak{p} \subset A$ um ideal primo e $B\mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i}$, onde os $\mathfrak{b}_i$ são ideais primos de B . Sabemos que um ideal primo $\mathfrak{p}$ de A que ramifica em B ou em L possui um dos seus índices de ramificação e_i maior que um. A seguir caracterizaremos os ideais primos de A que se ramificam em B usando a teoria de discriminante.

Lema 2.10.1 *Sejam A um anel, $\mathfrak{B}_1, \dots, \mathfrak{B}_q$ anéis contendo A , tais que sejam A -módulos livres finitamente gerados e seja $B = \prod_{i=1}^q \mathfrak{B}_i$ o produto de anéis. Então, $\mathfrak{D}_{B/A} = \prod_{i=1}^q \mathfrak{D}_{\mathfrak{B}_i/A}$.*

Demonstração: Faremos a demonstração por indução sobre q .

- Para $q = 2$, sejam $\{x_1, \dots, x_n\}$, $\{y_1, \dots, y_m\}$ as bases para os A -módulos livres $\mathfrak{B}_1$ e $\mathfrak{B}_2$. Fazendo a identificação natural de $\mathfrak{B}_1$ em $\mathfrak{B}_1 \times \{0\}$ e $\mathfrak{B}_2$ em $\{0\} \times \mathfrak{B}_2$, podemos considerar $\{x_1, \dots, x_n, y_1, \dots, y_m\}$ como uma base de $B = \mathfrak{B}_1 \times \mathfrak{B}_2$. Como pela própria estrutura do anel produto B temos $x_i y_j = 0, \forall i, j$, e portanto, $\text{Tr}(x_i y_j) = 0$.

Assim, $\mathfrak{D}(x_1, \dots, x_n, y_1, \dots, y_m) = \det \begin{pmatrix} \text{Tr}(x_i x_{i'}) & 0 \\ 0 & \text{Tr}(y_j y_{j'}) \end{pmatrix} = \det(\text{Tr}(x_i x_{i'})) \cdot \det(\text{Tr}(y_j y_{j'}))$, ou seja, $\mathfrak{D}(x_1, \dots, x_n, y_1, \dots, y_m) = \mathfrak{D}(x_1, \dots, x_n) \cdot \mathfrak{D}(y_1, \dots, y_m)$.

- Suponha que o resultado seja válido para $q - 1$, ou seja, se $B = \prod_{i=1}^{q-1} \mathfrak{B}_i$, então

$\mathfrak{D}_{B/A} = \prod_{i=1}^{q-1} \mathfrak{D}_{\mathfrak{B}_i/A}$. Sejam, $\mathfrak{C}_1 = \mathfrak{B}_1 \cdots \mathfrak{B}_{q-1}$ e $\mathfrak{C}_2 = \mathfrak{B}_q$ e,

$$x_{1n} = (x_{11}, x_{12}, \dots, x_{1n}) \quad \text{base de } \mathfrak{B}_1$$

$$x_{2m} = (x_{21}, x_{22}, \dots, x_{2m}) \quad \text{base de } \mathfrak{B}_2$$

$\vdots$

$$x_{(q-1)s} = (x_{(q-1)1}, x_{(q-1)2}, \dots, x_{(q-1)s}) \quad \text{base de } \mathfrak{B}_{q-1}$$

$$y_q = (y_{q1}, y_{q2}, \dots, y_{q_l}) \quad \text{base de } \mathfrak{B}_q$$

Fazendo as seguintes identificações $\mathfrak{C}_1 \rightarrow \mathfrak{C}_1 \times \{0\}$, $\mathfrak{C}_2 \rightarrow \{0\} \times \mathfrak{C}_2$ e considerando

$B = \mathfrak{C}_1 \times \mathfrak{C}_2$, temos que $\{x_{1n}, x_{2m}, \dots, x_{(q-1)s}, y_q\}$ é uma base de B e usando o caso

para $q = 2$, temos que $\mathfrak{D}_{B/A} = \mathfrak{D}_{\mathfrak{C}_1/A} \cdot \mathfrak{D}_{\mathfrak{C}_2/A} \stackrel{H.I.}{=} \prod_{i=1}^{q-1} \mathfrak{D}_{\mathfrak{B}_i/A} \cdot \mathfrak{D}_{\mathfrak{B}_q/A} = \prod_{i=1}^q \mathfrak{D}_{\mathfrak{B}_i/A}$. $\blacksquare$

Lema 2.10.2 *Sejam B um anel, A um subanel de B e $\mathfrak{a}$ um ideal de A . Se B é um A -módulo livre com base $\{x_1, \dots, x_n\}$, então $\{\overline{x_1}, \dots, \overline{x_n}\}$ é uma base de $B/\mathfrak{a}B$ sobre $A/\mathfrak{a}$ e $\mathfrak{D}(\overline{x_1}, \dots, \overline{x_n}) = \overline{\mathfrak{D}(x_1, \dots, x_n)}$.*

Demonstração: Da demonstração do Teorema 2.9.5 temos que $\{\overline{x_1}, \dots, \overline{x_n}\}$ é uma base de $B/\mathfrak{a}B$ sobre $A/\mathfrak{p}$. Sejam $x \in B$ e $m_x : B \rightarrow B$ o endomorfismo que a cada b associa xb com $M = [a_{ij}]$; $a_{ij} \in A$, a sua matriz. Agora seja $m_{\overline{x}} : B/\mathfrak{a}B \rightarrow B/\mathfrak{a}B$ o endomorfismo de

multiplicação por $\bar{x}$ que a cada $\bar{b}$ associa $\bar{x}\bar{b}$. Temos que $\overline{M} = [\overline{a_{ij}}]$, com $\overline{a_{ij}} \in A/\mathfrak{a}$, é sua matriz, uma vez que

$$m_{\bar{x}}(\bar{x}_1) = \bar{x} \bar{x}_1 = xx_1 + \mathfrak{a}B = (a_{11}x_1 + \cdots + a_{1n}x_n) + \mathfrak{a}B = (a_{11}x_1 + \mathfrak{a}B) + \cdots +$$

$$+ (a_{1n}x_n + \mathfrak{a}B) = \overline{a_{11}x_1} + \cdots + \overline{a_{1n}x_n}$$

...

$$m_{\bar{x}}(\bar{x}_n) = \bar{x} \bar{x}_n = xx_n + \mathfrak{a}B = (a_{n1}x_1 + \cdots + a_{nn}x_n) + \mathfrak{a}B = (a_{n1}x_1 + \mathfrak{a}B) + \cdots +$$

$$+ (a_{nn}x_n + \mathfrak{a}B) = \overline{a_{n1}x_1} + \cdots + \overline{a_{nn}x_n},$$

e portanto,

$$\overline{M} = \begin{pmatrix} \overline{a_{11}} & \cdots & \overline{a_{1n}} \\ \vdots & \vdots & \vdots \\ \overline{a_{n1}} & \cdots & \overline{a_{nn}} \end{pmatrix}.$$

Como $Tr(x) = \sum_i a_{ii} \Rightarrow Tr(\bar{x}) = \sum_i \overline{a_{ii}} = \overline{\sum_i a_{ii}} = \overline{Tr(x)}$, e se tomarmos $x = x_i x_j$, temos que $Tr(\overline{x_i x_j}) = \overline{Tr(x_i x_j)}$. Assim, $det(Tr(\overline{x_i x_j})) = \overline{det(Tr(x_i x_j))}$, ou seja, $\mathfrak{D}(\bar{x}_1, \dots, \bar{x}_n) = \overline{\mathfrak{D}(x_1, \dots, x_n)}$. $\blacksquare$

Definição 2.10.1 Seja A um anel. Dizemos que um elemento $a \in A$ é chamado **nilpotente** se existe $n \in \mathbb{N}$, tal que $a^n = 0$. Dizemos que um anel A é **reduzido** se o único elemento nilpotente de A é o 0.

Definição 2.10.2 Um espaço vetorial A sobre um corpo $\mathbb{K}$ é uma **$\mathbb{K}$ -álgebra** ou uma **álgebra sobre $\mathbb{K}$** se existe uma multiplicação:

$$\bullet : A \times A \longrightarrow A$$

$$(a, b) \longmapsto ab$$

satisfazendo,

1. $a(b + c) = ab + ac, \forall a, b, c \in A,$
2. $a(\alpha b) = (\alpha a)b = \alpha(ab), \forall \alpha \in \mathbb{K}, a, b \in A,$
3. $a(bc) = (ab)c, \forall a, b, c \in A,$
4. $\exists 1_A \in A; a1_A = a = 1_A a, \forall a \in A.$

♣ Se $ab = ba$, $\forall a, b \in A$, temos uma K -álgebra comutativa.

♠ Se, $\forall a \in A$; $a \neq 0, \exists a' \in A \mid aa' = 1_A$, dizemos que A é uma álgebra de divisão.

Lema 2.10.3 Em um anel Noetheriano reduzido A , o ideal (0) é expresso como a intersecção de um número finito de ideais primos de A .

Demonstração: Pelo Corolário 2.6.3, temos que todo ideal de um anel Noetheriano contém um produto de ideais primos. Como (0) é o menor ideal de A , segue que (0) é um produto de ideais primos de A , ou seja, $(0) = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q}$. Se $x \in \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_q$, então $x^{n_1 + \dots + n_q} \in \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_q^{n_q} = (0)$, e assim $x^{n_1 + \dots + n_q} = 0$. Como A é reduzido, temos que $x = 0$. Portanto, $(0) = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_q$, ou seja, o ideal (0) é expresso como a intersecção de um número finito de ideais primos de A . $\blacksquare$

Lema 2.10.4 Sejam K um corpo, L uma K -álgebra comutativa de dimensão finita. Então, L é um anel reduzido se, e somente se, $\mathfrak{D}_{L/K} \neq (0)$.

Demonstração: Se L é reduzido, então pelo Lema 2.10.3, temos que $(0) = \bigcap_{i=1}^q \mathfrak{b}_i$, com $\mathfrak{b}_i$'s ideais primos de L . Temos que $L/\mathfrak{b}_i$ é um domínio e uma K -álgebra de dimensão finita. Assim, $L/\mathfrak{b}_i$ é uma extensão algébrica, ou seja, todo elemento de $L/\mathfrak{b}_i$ é inteiro sobre $A/\mathfrak{p}$. Pela Proposição 2.1.3, segue que $L/\mathfrak{b}_i$ é corpo. Assim, $\mathfrak{b}_i$ é um ideal maximal de L , e conseqüentemente, $\mathfrak{b}_i + \mathfrak{b}_j = L$, para todo $i \neq j$. Assim, $\prod_{i=1}^q L/\mathfrak{b}_i = L/\mathfrak{b}_1 \cdots \mathfrak{b}_q = L/(0) = L$, e portanto, $\mathfrak{D}_{L/K} = \prod_{i=1}^q \mathfrak{D}_{(L/\mathfrak{b}_i)/K}$. Como $\mathfrak{D}_{(L/\mathfrak{b}_i)/K} \neq 0$, segue que $\mathfrak{D}_{L/K} \neq 0$. Por outro lado, suponha que L não seja reduzido, e seja $x \neq 0$ um elemento nilpotente de L . Seja $\{x_1, \dots, x_n\}$ uma base de L sobre K , tal que $x = x_1$. Então, $x_1 x_j, \forall j$, é nilpotente, e assim o endomorfismo $m_{x_1 x_j} : L \rightarrow L$ que a cada $l \in L$ associa $l x_1 x_j$, tem seus auto valores todos nulos, e portanto, $Tr(x_1 x_j) = 0$. Assim, a matriz $(Tr(x_i x_j))$ tem uma linha nula, o que implica que $\mathfrak{D}(x_1, \dots, x_n) = 0$, ou seja, $\mathfrak{D}_{L/K} = (0)$, o que é um absurdo. Logo a K -álgebra L é reduzido. $\blacksquare$

Teorema 2.10.1 Sejam K e L corpos de números, tal que $K \subset L$, $\mathcal{O}_K$ e $\mathcal{O}_L$ os anéis dos inteiros de K e L respectivamente, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$. Então, $\mathfrak{p}$ ramifica se, e somente se, $\mathcal{O}_L/\mathcal{O}_L \mathfrak{p}$ não é reduzido.

Demonstração: Seja $\mathcal{O}_L \mathfrak{p} = \prod_{i=1}^q \mathfrak{b}_i^{e_i}$, com $\mathfrak{b}_i \subset \mathcal{O}_L$ ideais primos, tal que $\mathfrak{b}_i \cap A = \mathfrak{p}$. Se $\mathfrak{p}$ se ramifica, então existe $k \in \mathbb{N}$, tal que $e_k > 1$. Temos que $\mathfrak{p}\mathcal{O}_L \subsetneq \mathfrak{b}_j$, $\forall j$, pois se $\mathfrak{p}\mathcal{O}_L = \mathfrak{b}_j$ teríamos $e_j = 1$ o que é contra hipótese. Para cada i , seja $a_i \in \mathfrak{b}_i \setminus \mathfrak{p}\mathcal{O}_L$ e seja $\bar{x} = a_1 \cdots a_k a_{k+1} \cdots a_q + \mathcal{O}_L \mathfrak{p} \neq \bar{0}$, com $a_1 \cdots a_q \in \mathcal{O}_L \setminus \mathcal{O}_L \mathfrak{p}$. Assim, se $r = e_1 \cdots e_q$, então $\bar{x}^r = (a_1 \cdots a_q)^r + \mathcal{O}_L \mathfrak{p} = a_1^r \cdots a_k^r a_{k+1}^r \cdots a_q^r + \mathcal{O}_L \mathfrak{p} = \mathfrak{B} \mathfrak{p} = \bar{0}$. Portanto, $\mathcal{O}_L / \mathcal{O}_L \mathfrak{p}$ não é reduzido. Por outro lado, como $\mathcal{O}_L / \mathcal{O}_L \mathfrak{p} \simeq \prod_{i=1}^q \mathcal{O}_L / \mathfrak{b}_i^{e_i}$ não é reduzido, existe $x \neq 0$, $x = (x_1 + \mathfrak{b}_1^{e_1}, \dots, x_q + \mathfrak{b}_q^{e_q}) \in \prod_{i=1}^q \mathcal{O}_L / \mathfrak{b}_i^{e_i}$, tal que x é nilpotente. Então, $\exists j$, tal que $x_j \notin \mathfrak{b}_j^{e_j}$ e $\exists n \in \mathbb{N}$, com $n > 1$, tal que $(x_1 + \mathfrak{b}_1^{e_1}, \dots, x_q + \mathfrak{b}_q^{e_q})^n = \bar{0} = (x_1^n + \mathfrak{b}_1^{e_1}, \dots, x_q^n + \mathfrak{b}_q^{e_q})$. Assim, $x_i^n \in \mathfrak{b}_i^{e_i}, \forall i = 1, \dots, q$, em particular $x_j^n \in \mathfrak{b}_j^{e_j}$. Se $e_j = 1$, então $x_j^n \in \mathfrak{b}_j$, e como $\mathfrak{b}_j$ é primo segue que, $x_j \in \mathfrak{b}_j$ o que é contra hipótese. Portanto, $e_j > 1$, ou seja, $\mathfrak{p}$ ramifica. $\blacksquare$

Corolário 2.10.1 *Sobre as mesmas condições do Teorema 2.10.1, temos que $\mathfrak{p}$ ramifica se, e somente se, $\mathfrak{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = (0)$.*

Demonstração: Pelo Teorema 2.10.1, temos que $\mathfrak{p}$ ramifica se, e somente se, $B/B\mathfrak{p}$ não é reduzido, e pelo Lema 2.10.4, $B/B\mathfrak{p}$ não é reduzido se, e somente se, $\mathfrak{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = (0)$. $\blacksquare$

Definição 2.10.3 *Sejam K e L corpos numéricos com $K \subset L$. Sejam $\mathcal{O}_K$ e $\mathcal{O}_L$ os anéis dos inteiros de K e L , respectivamente. O discriminante de $\mathcal{O}_L$ sobre $\mathcal{O}_K$ (ou de L sobre K) é o ideal de $\mathcal{O}_K$ gerado pelo discriminante das bases de L sobre K que estão contidas em $\mathcal{O}_L$. Notação: $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$ ou $\mathfrak{D}_{L/K}$.*

Observações 2.10.1 1) Se $\{x_1, \dots, x_n\}$ é uma base de L sobre K contida em $\mathcal{O}_L$, pelo Corolário 2.3.1, temos que $\text{Tr}(x_i x_j) \in \mathcal{O}_K$, e portanto $D(x_1, \dots, x_n) \in \mathcal{O}_K$, ou seja, $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$ é um ideal de $\mathcal{O}_K$. Além disso, é não nulo pela Proposição 2.4.3.

2) Se $\mathcal{O}_L$ é um $\mathcal{O}_K$ -módulo livre, temos pela Definição 2.4.2 que o discriminante $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$ é o ideal gerado $D(e_1, \dots, e_n)$, onde $\{e_1, \dots, e_n\}$ é uma base de $\mathcal{O}_L$. Agora, se $\{x_1, \dots, x_n\}$ é uma base de L sobre K contida em $\mathcal{O}_L$, temos que $x_i = \sum_{j=1}^n a_{ij} e_j$, com $a_{ij} \in \mathcal{O}_K$, e pela Proposição 2.4.1, segue que $D(x_1, \dots, x_n) = \det(a_{ij})^2 D(e_1, \dots, e_n)$, o que mostra que as duas definições são equivalentes. $\blacksquare$

Teorema 2.10.2 *Sejam K e L corpos de números, tal que $K \subset L$, $\mathcal{O}_K$ e $\mathcal{O}_L$ os anéis dos inteiros de K e L respectivamente, e $\mathfrak{p}$ um ideal primo não nulo de A . Então, $\mathfrak{p}$ ramifica se, e somente se, $\mathfrak{p} \supset \mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$.*

Demonstração: Suponhamos que $\mathfrak{p}$ ramifica. Fazendo $S = \mathcal{O}_K - \mathfrak{p}$, temos que $\mathfrak{A} = S^{-1}\mathcal{O}_K$, $\mathfrak{B} = S^{-1}\mathcal{O}_L$ e $\mathfrak{p}' = \mathfrak{p}\mathfrak{A}$. Pelo Teorema 2.9.3, temos que $\mathfrak{A}$ é um anel principal, $\mathfrak{B}$ é um $\mathfrak{A}$ -módulo livre, $\mathcal{O}_K/\mathfrak{p} \simeq \mathfrak{A}/\mathfrak{p}'$ e $\mathcal{O}_L/\mathfrak{B}\mathfrak{p} \simeq \mathfrak{B}/\mathfrak{B}\mathfrak{p}'$. Se $\{e_1, \dots, e_n\}$ é uma base de $\mathfrak{B}$, pelo Corolário 2.10.1, temos que $\mathfrak{D}_{(\mathcal{O}_L/\mathcal{O}_L\mathfrak{p})/(\mathcal{O}_K/\mathfrak{p})} = (0) \iff D(e_1, \dots, e_n) \in \mathfrak{p}'$. Mas se $D(e_1, \dots, e_n) \in \mathfrak{p}'$ e se $\{x_1, \dots, x_n\}$ é uma base de L sobre K contida em $\mathcal{O}_L$, temos $x_i = \sum_{j=1}^n a'_{ij} e_j$, com $a'_{ij} \in \mathfrak{A}$, pois $\mathcal{O}_L \subset \mathfrak{B}$. Assim, $D(x_1, \dots, x_n) \in \mathcal{O}_K$ e $D(x_1, \dots, x_n) = (\det(a'_{ij}))^2 D(e_1, \dots, e_n) \in \mathfrak{p}'$, e portanto, $D(x_1, \dots, x_n) \in \mathfrak{p}' \cap \mathcal{O}_K = \mathfrak{p}$. Portanto, $\mathfrak{D}_{\mathfrak{B}/\mathcal{O}_K} = \langle D(x_1, \dots, x_n) \rangle \subset \mathfrak{p}$. Por outro lado, se $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} \subset \mathfrak{p} \xrightarrow{\mathcal{O}_K/\mathfrak{p} \simeq \mathfrak{A}/\mathfrak{p}'} D(e_1, \dots, e_n) \in \mathfrak{p}'$, onde $\{e_1, \dots, e_n\}$ é base de $\mathfrak{B}$. Assim, $e_i = \frac{y_i}{s}$, com $y_i \in B$ e $s \in S$, e portanto $\{y_1, \dots, y_n\}$ é uma base de L sobre K contida em $\mathcal{O}_L$. Mas $D(e_1, \dots, e_n) = \det(\text{Tr}(e_i e_j)) = \det(\text{Tr}\left(\frac{y_i y_j}{s^2}\right)) = \frac{1}{s^{2n}} \det(\text{Tr}(y_i y_j)) = s^{-2n} D(y_1, \dots, y_n) \in \mathfrak{A}$, ou seja, $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} \subset \mathfrak{A}\mathfrak{p} = \mathfrak{p}'$. Então, $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K} = (0)$, e pelo Corolário 2.10.1, segue que $\mathfrak{p}$ ramifica. Portanto, $\mathfrak{p}$ ramifica se, e somente se, $\mathfrak{p}$ contém $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$. $\blacksquare$

Corolário 2.10.2 *Com as notações do Teorema 2.10.2, temos que existe somente um número finito de ideais de $\mathcal{O}_K$ que se ramificam em $\mathcal{O}_L$.*

Demonstração: O resultado segue da fatoração do ideal de $\mathcal{O}_K$ gerado por $\mathfrak{D}_{\mathcal{O}_L/\mathcal{O}_K}$. $\blacksquare$

Exemplo 2.10.1 *Seja $K = \mathbb{Q}(\sqrt{d})$ com $d \in \mathbb{Z}$ livre de quadrados. Se $d \equiv 2$ ou $3 \pmod{4}$, então $\mathbb{Z}(\sqrt{d})$ é o anel dos inteiros de K . Como $\text{Tr}(1) = 2$, $\text{Tr}(\sqrt{d}) = 0$ e $\text{Tr}(d) = 2d$, segue que $D(1, \sqrt{d}) = 4d$. Assim, os primos que se ramificam em K é o 2 e os divisores de d . Agora, se $d \equiv 1 \pmod{4}$, então $\mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$ é o anel dos inteiros de K . Como $\text{Tr}(1) = 2$, $\text{Tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1$ e $\text{Tr}\left(\frac{1+\sqrt{d}}{2}\right)^2 = \text{Tr}\left(\frac{d+1}{4} + \frac{1}{2}\sqrt{d}\right) = \frac{d+1}{2}$, segue que $D\left(1, \frac{1+\sqrt{d}}{2}\right) = 2\frac{d+1}{2} - 1 = d$. Assim, os primos que se ramificam em L são os divisores de d . $\blacksquare$*



Proposição 2.10.1 *Seja ξ uma raiz n -ésima primitiva da unidade. Se p primo não divide n , então p não ramifica em $\mathbb{Q}(\xi)$.*

Demonstração: Seja $f(X)$ o polinômio minimal de ξ sobre $\mathbb{Q}$ e seja $n = [\mathbb{Q}(\xi) : \mathbb{Q}]$. Como $f(X)$ divide $X^n - 1$, temos que $X^n - 1 = f(X)g(X)$. Pela Proposição 2.4.4 temos que $D(1, \xi, \dots, \xi^{n-1}) = \pm \mathcal{N}(f'(\xi))$. Agora, como $nX^{n-1} = f'(X)g(X) + f(X)g'(X)$, segue que $n\xi^{n-1} = f'(\xi)g(\xi)$ uma vez que $f(\xi) = 0$. Como ξ é uma raiz da unidade, ou seja, $\mathcal{N}(\xi) = \pm 1$, segue que $\pm n^m = \mathcal{N}(f'(\xi))\mathcal{N}(g(\xi))$, e portanto, $\mathcal{N}(f'(\xi))$ divide n^m . Além disso, como ξ é inteiro sobre $\mathbb{Z}$, temos que o discriminante de $\mathbb{Q}(\xi)$ divide $D(1, \xi, \dots, \xi^{n-1})$, e portanto, também divide n^m . Finalmente, o resultado segue do Teorema 2.10.2. $\blacksquare$

O seguinte resultado é muitas vezes útil para determinar o anel dos inteiros de um corpo de números.

Proposição 2.10.2 *Sejam K um corpo de números de grau n , $\{x_1, \dots, x_n\}$ uma base de K sobre $\mathbb{Q}$ contida no anel $\mathcal{O}_K$ dos inteiros de K . Se o discriminante $D(x_1, \dots, x_n)$ é livre de quadrados, então $\{x_1, \dots, x_n\}$ é uma base de $\mathcal{O}_K$ sobre $\mathbb{Z}$.*

Demonstração: Se $\{e_1, \dots, e_n\}$ é uma base de $\mathcal{O}_K$ sobre $\mathbb{Z}$, então $x = \sum_{i=1}^n a_{ij}e_j$, com $a_{ij} \in \mathbb{Z}$. Pela Proposição 2.4.1, temos que $D(x_1, \dots, x_n) = (\det(a_{ij}))^2 D(e_1, \dots, e_n)$. Como $D(x_1, \dots, x_n)$ é livre de quadrados, segue que $\det(a_{ij}) = \pm 1$, ou seja, $\{x_1, \dots, x_n\}$ também é uma base de $\mathcal{O}_K$ sobre $\mathbb{Z}$. $\blacksquare$

Exemplo 2.10.2 *O polinômio $X^3 + X + 1$ é irredutível sobre $\mathbb{Q}$. Seja $x \in \mathbb{C}$ uma raiz, e portanto x é inteiro. Temos que $K = \mathbb{Q}[x]$ é uma extensão cúbica de $\mathbb{Z}$ e $\{1, x, x^2\}$ é uma base de $\mathbb{L}/K$ sobre $\mathbb{Q}$. Assim, $D(1, x, x^2) = -23$, que é livre de quadrados, e portanto, $\{1, x, x^2\}$ é uma base $\mathbb{L}/K$ sobre $\mathbb{Z}$. $\blacksquare$*

Capítulo 3

Reticulados

Neste Capítulo faremos um estudo sobre reticulados via homomorfismo de Minkowski no $\mathbb{R}^n$, definindo seus principais parâmetros, tais como região fundamental, empacotamento esférico, densidade de empacotamento e densidade de centro. Através do homomorfismo canônico obtemos um método de gerar reticulados no $\mathbb{R}^n$. Os reticulados obtidos desta maneira dependem diretamente do anel dos inteiros de um corpo de números. O grande desafio é encontrar o anel dos inteiros de qualquer corpo numérico, uma vez que são conhecidos apenas o anel dos inteiros dos corpos quadráticos e dos corpos ciclotômicos. Assim, para obtermos bons reticulados no $\mathbb{R}^n$, via o homomorfismo de Minkowski, primeiramente necessitamos do conhecimento do anel dos inteiros de um corpo de números de grau n . Deste modo, no presente Capítulo faremos um estudo sobre reticulados no $\mathbb{R}^n$, sobre empacotamento esférico, explicitaremos alguns reticulados construtivos conhecidos na literatura e obtenção de reticulados via o homomorfismo canônico.

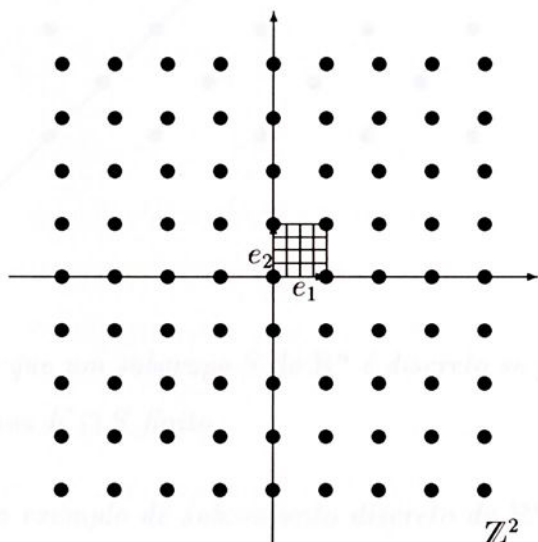
3.1 Reticulados

Sejam V um espaço vetorial de dimensão finita n sobre um corpo $\mathbb{L}$, A um subanel de $\mathbb{L}$ e $v_1, \dots, v_m$, vetores de V linearmente independentes sobre $\mathbb{L}$, com $m \leq n$. Dá-se o nome de **reticulado** com base $\beta = \{v_1, \dots, v_m\}$ ao conjunto dos elementos de V do tipo, $\lambda = \sum_{i=1}^m a_i v_i$, com $a_i \in A$, que será denotado por Λ_β .

$$T_v = \left\{ \sum_{i=1}^m \rho_i v_i \mid 0 \leq \rho_i < 1; i = 1, \dots, m \right\}.$$

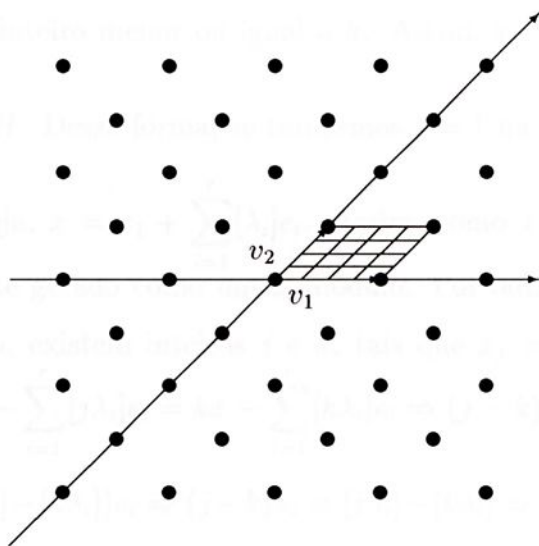
Dizemos que T_v é a **região fundamental** do reticulado Λ associada a base β . Se $n = m$, dizemos que o reticulado Λ_β é um **reticulado completo** e que $\{v_1, \dots, v_n\}$ é uma base completa do reticulado.

Exemplo 3.1.1 Temos que $\Lambda_\beta = \mathbb{Z}^2$ é um reticulado completo do $\mathbb{R}^2$ gerado pela base $\beta = \{e_1 = (1, 0), e_2 = (0, 1)\}$, com região fundamental descrita na figura abaixo.



$\mathbb{Z}^2$

Exemplo 3.1.2 Temos que, $\Lambda_\beta = \{(a, b) \in \mathbb{Z}^2; a + b \equiv 0 \pmod{2}\}$ é um reticulado completo do $\mathbb{R}^2$ gerado pela base $\beta = \{v_1 = (2, 0), v_2 = (1, 1)\}$, com região fundamental descrita na figura abaixo.



Definição 3.1.1 Dizemos que um subgrupo S do $\mathbb{R}^n$ é discreto se para qualquer subconjunto compacto K do $\mathbb{R}^n$, tivermos $K \cap S$ finito.

Exemplo 3.1.3 Um típico exemplo de subconjunto discreto do $\mathbb{R}^n$ é $\mathbb{Z}^n$.

O próximo teorema nos diz que um reticulado é gerado sobre $\mathbb{Z}$ por uma base do $\mathbb{R}^n$, a qual é então, uma $\mathbb{Z}$ -base do reticulado dado.

Teorema 3.1.1 Seja H um subgrupo discreto do $\mathbb{R}^n$. Então, H é gerado como um $\mathbb{Z}$ -módulo por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.

Demonstração: Seja $\{e_1, \dots, e_r\}$ um conjunto de elementos de H linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível com $r \leq n$.

Seja $\mathcal{P} = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^r \alpha_i e_i, 0 \leq \alpha_i \leq 1 \right\}$ um paralelepípedo construído a partir destes vetores. Temos que $\mathcal{P}$ é compacto e como H é discreto, segue que $\mathcal{P} \cap H$ é finito. Para

qualquer $x \in H$, pela maximalidade de r , temos que $x = \sum_{i=1}^r \lambda_i e_i$, $\lambda_i \in \mathbb{R}$. Consideremos $j \in \mathbb{Z}$, e seja:

$$x_j = jx - \sum_{i=1}^r [j\lambda_i] e_i, \quad (3.1.1)$$

onde $[k]$ denota o maior inteiro menor ou igual a k . Assim, $x_j = j \sum_{i=1}^r \lambda_i e_i - \sum_{i=1}^r [j\lambda_i] e_i =$

$\sum_{i=1}^r (j\lambda_i - [j\lambda_i]) e_i \in \mathcal{P} \cap H$. Dessa forma, se tomarmos $j = 1$ na equação (3.1.1) temos que

$x_1 = x - \sum_{i=1}^r [\lambda_i] e_i$, ou seja, $x = x_1 + \sum_{i=1}^r [\lambda_i] e_i$. Assim, como $x_1 \in \mathcal{P} \cap H$ e este é finito,

segue que H é finitamente gerado como um $\mathbb{Z}$ -módulo. Por outro lado, do fato de $\mathcal{P} \cap H$ ser finito e $\mathbb{Z}$ ser infinito, existem inteiros j e k , tais que $x_j = x_k$. Da equação (3.1.1),

segue que $x_j = x_k \Rightarrow jx - \sum_{i=1}^r [j\lambda_i] e_i = kx - \sum_{i=1}^r [k\lambda_i] e_i \Rightarrow (j-k)x = \sum_{i=1}^r ([j\lambda_i] - [k\lambda_i]) e_i \Rightarrow$

$(j-k) \sum_{i=1}^r \lambda_i e_i = \sum_{i=1}^r ([j\lambda_i] - [k\lambda_i]) e_i \Rightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i] \Rightarrow \lambda_i = \frac{[j\lambda_i] - [k\lambda_i]}{(j-k)}$, ou seja,

λ_i pertence a $\mathbb{Q}$. Assim, H é gerado como um $\mathbb{Z}$ -módulo por um número finito de elementos,

que são combinações lineares com coeficientes racionais dos e_i 's. Seja $d \neq 0$ um denominador comum destes coeficientes. Consideremos o conjunto dH . Temos que $dH \subset \sum_{i=1}^r \mathbb{Z} e_i$. Daí,

pelo Teorema 1.1.3, segue que existe uma base $(f_1, \dots, f_r)$ do $\mathbb{Z}$ -módulo $\sum_{i=1}^r \mathbb{Z} e_i$ e inteiros α_i , tal que $\{\alpha_1 f_1, \dots, \alpha_r f_r\}$ gera dH . Deste modo, o $\mathbb{Z}$ -módulo dH tem o mesmo posto de

H e como $\sum_{i=1}^r \mathbb{Z} e_i \subset H$, temos que o posto de $dH \geq r$. Pela maximalidade de r decorre que o posto de dH é r e os α_i 's são não nulos, pois caso contrário dH não teria posto r .

Assim, os f_i 's são linearmente independentes sobre $\mathbb{R}$. Portanto, dH é gerado por r vetores

linearmente independentes sobre $\mathbb{R}$ e conseqüentemente H também é gerado por r vetores

linearmente independentes sobre $\mathbb{R}$. ■

Dado um reticulado H , além da região fundamental T_v , existem também outras regiões $z + T_v$, com $z \in H$, associadas a uma base $\{v_1, \dots, v_m\}$ do reticulado H . Veremos a seguir que todo conjunto limitado intersecta apenas um número finito destas regiões.

Proposição 3.1.1 *Seja T_v a região fundamental associada a base $v_1, \dots, v_m$ de um reticulado H e seja C um subconjunto limitado de $\mathbb{L}$. Então, $C \cap (z + T_v) = \emptyset$, para quase todos*

os pontos z de H .

Demonstração: Para todo $t \in T_v$, temos que $t = \sum_{i=1}^m \rho_i v_i$ e $\|T\| = \|\sum_{i=1}^m \rho_i v_i\| \leq \sum_{i=1}^m \|\rho_i v_i\| = \sum_{i=1}^m |\rho_i| \cdot \|v_i\| \leq \sum_{i=1}^m \|v_i\| = \tau$. Suponhamos sem perda de generalidade que $C = B_\rho$ (bola de centro 0 e raio ρ), para algum $\rho \geq 0$. Seja $z \in Z$, tal que $B_\rho \cap (z + T_v) \neq \emptyset$. Assim, $z + t = x \in B_\rho$ para algum $t \in T_v$, e portanto, $\|z\| = \|x - t\| \leq \|x\| + \|t\| \leq \rho + \tau$, ou seja, $z \in B_{\rho+\tau}$. Como H é discreto, temos que o conjunto $H \cap B_{\rho+\tau}$ é finito. Assim, existem finitos pontos de H que pertencem a $B_{\rho+\tau}$, e portanto, existem finitos pontos de H , tal que $B_{\rho+\tau} \cap (z + T_v) \neq \emptyset$, uma vez que se $B_\rho \subset B_{\rho+\tau}$, segue que $B_\rho \cap (z + T_v) \neq \emptyset$ para um número finito de $z \in H$. $\blacksquare$

Quanto aos reticulados completos, é intuitivamente claro que a reunião de todas as regiões associadas a uma base de um reticulado completo cobre todo o espaço $\mathbb{L}$, e que os reticulados completos podem ser caracterizados por uma propriedade mais fraca, a saber pela existência de um conjunto limitado C , tal que $\bigcup_{z \in H} (z + C) = \mathbb{L}$.

Teorema 3.1.2 *Seja H um reticulado de $\mathbb{L}$. As seguintes condições são equivalentes.*

(i) H é um reticulado completo de $\mathbb{L}$.

(ii) Existe um subconjunto limitado C de $\mathbb{L}$ tal que $\mathbb{L} = \bigcup_{z \in H} (z + C)$. Em particular, temos que $\mathbb{L} = \bigcup_{z \in H} (z + T)$ (reunião disjunta), sendo T a região fundamental associada a uma base de H .

Demonstração: (i) $\Rightarrow$ (ii) Para todo $x \in \mathbb{L}$, temos que $x = \sum_{i=1}^n a_i v_i + \sum_{i=1}^n \rho_i v_i$ com $a_i \in \mathbb{Z}$ e $0 \leq \rho_i < 1$, $i = 1, \dots, n$. Assim, temos que $\mathbb{L} \subset \bigcup_{z \in H} (z + T_v)$, e como a inclusão contrária é imediata, segue que $\mathbb{L} = \bigcup_{z \in H} (z + T_v)$. Esta união é disjunta, pois se tivermos

$\sum_{i=1}^n a_i v_i + \sum_{i=1}^n \rho_i v_i = \sum_{i=1}^n a'_i v_i + \sum_{i=1}^n \rho'_i v_i$, segue que $\sum_{i=1}^n (a_i - a'_i) v_i = \sum_{i=1}^n (\rho'_i - \rho_i) v_i$, e então $a_i - a'_i = \rho'_i - \rho_i$, ou seja, $a_i + \rho_i = a'_i + \rho'_i$, $\forall i = 1, \dots, n$, e portanto, $a_i = a'_i$ e $\rho_i = \rho'_i$.

(ii) $\Rightarrow$ (i) Suponhamos que H não seja um reticulado completo. Seja $\{u_1, \dots, u_m\}$ uma base de H com $m < n$. Então, podemos completar esta base a uma base $\{u_1, \dots, u_{m+1}, \dots, u_n\}$ do espaço $\mathbb{L}$. Se $\{w_1, \dots, w_n\}$ é a base dual de $\{u_1, \dots, u_n\}$, então o produto interno

$\langle z, w_n \rangle = 0, \forall z \in H$, com $z = \sum_{i=1}^n a_i u_i$. Suponhamos, sem perda de generalidade, que $\|w_n\| = 1$. Seja $\rho > 0$, tal que $C \subseteq B_\rho$, e seja $y = \rho' w_n$ para algum $\rho' > \rho$. Por hipótese, temos que $y = z + c$, com $c \in C$ e $z \in H$. Como $\langle z, y \rangle = 0$, concluímos que $\|y\|^2 = \langle z + c, y \rangle = \langle z, y \rangle + \langle c, y \rangle \leq \|c\| \|y\| \leq \rho \|y\|$, ou seja, $\|y\| \leq \rho$, o que contradiz o fato de $\|y\| = \|\rho' w_n\| = \rho'$. $\blacksquare$

Para que possamos prosseguir no estudo de reticulados completos de $\mathbb{L}$, precisamos da noção de volume em $\mathbb{L}$. O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$ -espaço $\mathbb{L}$ através do isomorfismo natural entre $\mathbb{R}^n$ e $\mathbb{L}$, e definido por meio da base canônica $\{e_1, \dots, e_n\}$. Além disso, é possível se restringir a subconjuntos C de $\mathbb{L}$ que são reuniões finitas de paralelepípedos, usando apenas as seguintes propriedades de volume.

- a) $\text{Vol}(T_v) = |\det(\alpha_{ij})|$, sendo $v_i = \sum_{j=1}^n \alpha_{ij} e_j, \alpha_{ij} \in \mathbb{R}, i = 1, \dots, n$.
- b) $\text{Vol}(x + C) = \text{Vol}(C)$, para todo $x \in \mathbb{L}$.
- c) $\text{Vol}(\gamma C) = \gamma^n \text{Vol}(C)$, para todo $\gamma \in \mathbb{R}, \gamma > 0$.
- d) Se $C \cap C' = \emptyset$, então $\text{Vol}(C \cup C') = \text{Vol}(C) + \text{Vol}(C')$.

Proposição 3.1.2 *O volume da região fundamental $\text{Vol}(T_v)$ é independente da base v de H .*

Demonstração: Seja $f = \{f_1, \dots, f_n\}$ uma outra base de H . Então, $f_i = \sum_{j=1}^n \alpha_{ij} v_j$, com $\alpha_{ij} \in \mathbb{Z}$. Assim, $\text{Vol}(T_v) = |\det(\alpha_{ij})| \text{Vol}(T_v)$. Como a matriz de mudança de base (α_{ij}) é invertível, segue que $\det(\alpha_{ij}) = \pm 1$. Portanto, $\text{Vol}(T_f) = \text{Vol}(T_v)$. $\blacksquare$

Definição 3.1.2 *O volume do paralelepípedo T_v associado com uma base v de H é chamado de volume do reticulado H .*

Teorema 3.1.3 *Seja $C \subseteq \mathbb{L}$, tal que $\text{Vol}(C)$ seja definido e seja H um reticulado completo de $\mathbb{L}$. Se os conjuntos $z + C$, com $z \in H$ forem disjuntos dois a dois, então $\text{Vol}(C) \leq \text{Vol}(H)$.*

Demonstração: Seja T a região fundamental associada a uma base de H . Pelo Teorema 3.1.2, temos $\mathbb{L} = \bigcup_{z \in H} (z + T)$, e deste modo temos que $C = \bigcup_{z \in H} (C \cap (z + T))$ é também uma reunião disjunta. Pela Proposição 3.1.1, segue que existem $z_1, \dots, z_r$ em H , tais que $C \cap (z + T) = \emptyset$ para todo $x \in H \setminus \{z_1, \dots, z_r\}$. Assim, $\bigcup_{i=1}^r (C \cap (z_i + T))$ é uma reunião disjunta. Por hipótese, temos que $z_i + C$ são dois a dois disjuntos e como H é um subgrupo,

segue que os $-z_i + C$ também são dois a dois disjuntos, e portanto, a reunião $\bigcup_{i=1}^r (-z_i + C) \cap T$ também é disjunta. Disto, segue que $C \cap (z_i + T) = (-z_i + C \cap T) + z_i$. Assim, temos que

$$\text{Vol}(C) = \sum_{i=1}^r \text{Vol}(C \cap (z_i + T)) = \sum_{i=1}^r \text{Vol}((-z_i + C) \cap T) = \text{Vol}(\bigcup_{i=1}^r (-z_i + C) \cap T) \leq \text{Vol}(T) = \text{Vol}(H).$$

■

Teorema 3.1.4 *Sejam H um reticulado de posto n no $\mathbb{R}^n$ e S um subconjunto do $\mathbb{R}^n$, com $\text{Vol}(S)$ definido e tal que $\text{Vol}(S) > \text{Vol}(H)$. Então, existem dois pontos distintos $x, y \in S$, tal que $x - y \in H$.*

Demonstração: Seja $e = \{e_1, \dots, e_n\}$ uma $\mathbb{Z}$ -base de H e seja T_e a região fundamental de H . Assim, S é a união disjunta de subconjuntos da forma $S \cap (h + T_e)$; $h \in H$, e portanto,

$$\text{Vol}(S) = \sum_{h \in H} \text{Vol}(S \cap (h + T_e)). \quad (3.1.2)$$

Como o volume é invariante por translação, temos que $\text{Vol}(S \cap (h + T_e)) = \text{Vol}((-h + S) \cap T_e)$. Os conjuntos $(-h + S) \cap T_e$ não podem ser todos dois a dois disjuntos, pois caso contrário $\text{Vol}(T_e) \geq \sum \text{Vol}((-h + S) \cap T_e)$, o que contradiz a hipótese. Logo, existem dois elementos distintos $h, h' \in H$, tais que $((-h + S) \cap T_e) \cap ((-h' + S) \cap T_e) = T_e \cap (-h + S) \cap (-h' + S) \neq \emptyset$. Sejam $x, y \in S$ tais que $-h + x = -h' + y$. Então, $x - y = -h' + h \in H$ e $x \neq y$, uma vez que $h \neq h'$. ■

Teorema 3.1.5 *Sejam H um reticulado no $\mathbb{R}^n$, S um subconjunto do $\mathbb{R}^n$, cujo $\text{Vol}(S)$ é definido, e S é simétrico com respeito a origem e convexo. Se tivermos $\text{Vol}(S) > 2^n \text{Vol}(H)$, então $S \cap (H - \{0\}) \neq \emptyset$.*

Demonstração: Como $\text{Vol}\left(\frac{1}{2}S\right) = 2^{-n} \text{Vol}(S) > \text{Vol}(H)$, segue do Teorema 3.1.4 que os conjuntos $\frac{1}{2}S + z$ não são disjuntos dois a dois, isto é, existem $z_1, z_2 \in H$ com $z_1 \neq z_2$ e $c_1, c_2 \in S$, tais que $\frac{1}{2}c_1 + z_1 = \frac{1}{2}c_2 + z_2$. Como S é convexo e simétrico, temos que $-c_1 \in S$ e $z_1 - z_2 = \frac{1}{2}c_2 + (1 - \frac{1}{2})c_1 \in S \cap H - \{0\}$, como queríamos. ■

Teorema 3.1.6 *Sejam H um reticulado no $\mathbb{R}^n$, S um subconjunto do $\mathbb{R}^n$, cujo $\text{Vol}(S)$ é definido, e S é simétrico com respeito a origem e convexo. Se $\text{Vol}(S) > 2^n \text{Vol}(H)$ e S compacto, então $S \cap (H - \{0\}) \neq \emptyset$.*

Demonstração: Seja o conjunto $(1 + \epsilon)S$; $\epsilon > 0$. Então, $(1 + \epsilon)S$ é compacto, convexo e simétrico, e $\text{Vol}((1 + \epsilon)S) > 2^n \text{Vol}(H)$. Pelo Teorema 3.1.5, segue que $(1 + \epsilon)S \cap (H - \{0\}) \neq \emptyset$. Como H é discreto, segue que $(1 + \epsilon)S \cap (H - \{0\})$ é finito, e portanto, é compacto. Agora, temos que $(1 + \epsilon)S \subset (1 + \delta)S$ para $\delta > \epsilon$, uma vez que se $(1 + \epsilon)x \in (1 + \epsilon)S$, com $x \in S$, então $(1 + \epsilon)x = (1 + \delta)y \in S$, com $y \in S$ se, e somente se, $y = \left(\frac{1 + \epsilon}{1 + \delta}\right)x$, ou seja, $y = rx$, com $0 < r < 1$. Assim, é suficiente mostrar que $rx \in S$, para todo $0 < r < 1$. Como S é convexo, temos que $(1 - t)(-x) + tx \in S$, para todo $0 \leq t \leq 1$. Em particular, se $t = \frac{r+1}{2}$, temos que $\left(1 - \frac{r+1}{2}\right)(-x) + \left(\frac{r+1}{2}\right)x = rx \in S$. Assim, concluímos que $(1 + \epsilon)S \subset (1 + \delta)S$, para todo $\delta > \epsilon$. Pelo Teorema dos Intervalos Encaixantes, segue que $\bigcap_{\epsilon > 0} (H - \{0\}) \cap (1 + \epsilon)S \neq \emptyset$. Assim, existe $x \in (H - \{0\}) \cap (1 + \epsilon)S$, para todo $\epsilon > 0$.

Finalmente, temos que $(x_n) = \left(\frac{x}{1 + \frac{1}{n}}\right)$ é uma seqüência convergente de S , e como S é compacto, segue que (x_n) converge para $x \in S$. Portanto, $S \cap (H - \{0\}) \neq \emptyset$. $\blacksquare$

3.2 Empacotamento esférico

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. Um **empacotamento reticulado** é um empacotamento em que o conjunto dos centros formam um reticulado Λ_β do $\mathbb{R}^n$.

Fazendo $v_i = \{v_{i1}, \dots, v_{in}\}$, $i = 1, \dots, n$; temos que **volume** de Λ_β denotado por $v(\Lambda_\beta)$ é igual ao módulo do determinante da seguinte matriz, chamada de matriz geradora de Λ_β ,

$$B = \begin{pmatrix} v_{11} & \dots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{n1} & \dots & v_{nn} \end{pmatrix}.$$

Sendo β' uma outra base para Λ_β , segue que $v(\Lambda_\beta) = v(\Lambda_{\beta'})$, pois β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Assim, podemos definir o volume de Λ_β como sendo o volume de uma região fundamental.

O interessante são os empacotamentos associado a reticulados Λ_β em que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção

do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq k\}$ com o reticulado Λ_β é um conjunto finito, de onde segue que o número $\Lambda_{\beta_{min}} = \min\{|\lambda|; \lambda \in \Lambda_\beta, \lambda \neq 0\}$ está bem definido, e $(\Lambda_{\beta_{min}})^2$ é chamado **norma mínima**.

Observamos que $\rho = \Lambda_{\beta_{min}}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ_β e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados.

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

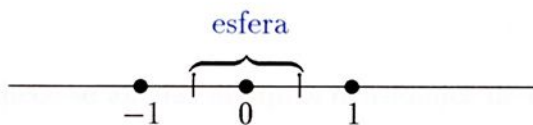
$$\Delta(\Lambda_\beta) = \frac{\text{Volume da região coberta pelas esferas}}{\text{Volume da região fundamental}} = \frac{v(B(\rho))}{v(\Lambda_\beta)} = \frac{v(B(1))\rho^n}{v(\Lambda_\beta)}.$$

Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de **densidade de centro**, que é dado por $\delta(\Lambda_\beta) = \frac{\rho^n}{v(\Lambda_\beta)}$.

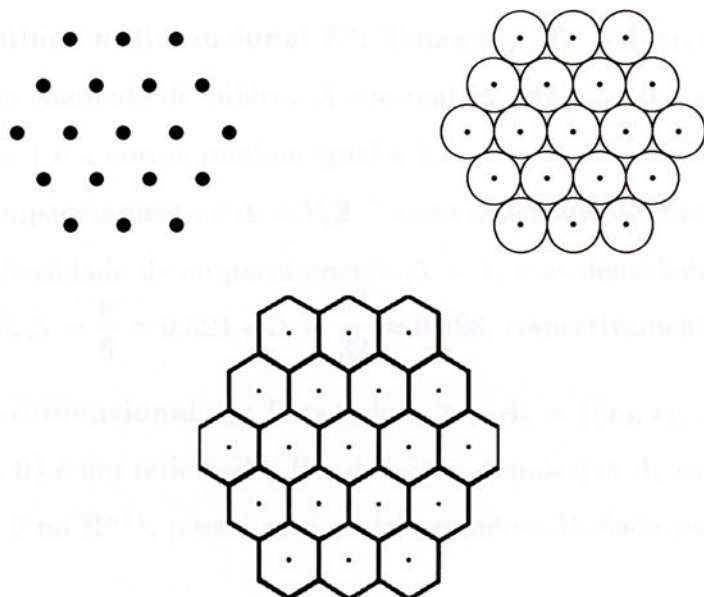
Exemplo 3.2.1 *Seja $\Lambda_\beta = \mathbb{Z}^n$ um reticulado do $\mathbb{R}^n$, gerado pela base $\beta = \{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1)\}$, temos que $\Lambda_{\beta_{\min}} = 1$, daí $\rho = \frac{1}{2}$. Visto que $v(\Lambda_\beta) = |\det B|$, e B neste caso é a matriz identidade, temos que $v(\Lambda_\beta) = 1$, e portanto, $\delta(\Lambda) = \frac{1}{2^n}$.*

Um dos problemas de empacotamento esférico de um reticulado Λ_β do $\mathbb{R}^n$ é encontrar um empacotamento com maior densidade.

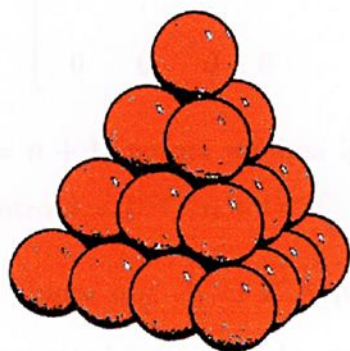
Em dimensão um, temos que os pontos de coordenadas inteiras da reta formam um $\mathbb{Z}$ -reticulado cuja a densidade de empacotamento é a melhor possível dada por $\Delta = 1$. Neste caso as “esferas” são segmentos de retas como podemos ver na figura abaixo.



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



Em dimensão três Gauss mostrou em 1831 que o reticulado *fcc* é o empacotamento com maior densidade (pirâmides de laranjas), sendo essa $\Delta = \frac{\pi}{\sqrt{18}} \approx 0,7405$.



Já para dimensões $n \geq 4$ conhece-se apenas algumas densidades de determinados empacotamentos, mais ainda não se sabe qual a melhor densidade.

3.3 Reticulados importantes e suas propriedades

Nesta seção descreveremos as propriedades de alguns reticulados construtivos importantes conhecidos na literatura.

Definição 3.3.1 Dizemos que um reticulado é equivalente a outro se este pode ser obtido do outro por rotação ou translação.

1. **Reticulado cúbico n -dimensional $\mathbb{Z}^n$:** Temos que, $\mathbb{Z}^n = \{(x_1, x_2, \dots, x_n); x_i \in \mathbb{Z}\}$ é um reticulado chamado de cúbico. A sua matriz geradora B é a matriz identidade. Assim, $\det \mathbb{Z}^n = 1$ e a norma mínima igual a 1, o raio de empacotamento é $\rho = \frac{1}{2}$, sua densidade de empacotamento é $\Delta = V_n 2^{-n}$ e sua densidade de centro é $\delta = 2^{-n}$. Desta forma $\mathbb{Z}$ tem densidade de empacotamento $\Delta = 1$, e as densidades de $\mathbb{Z}^2, \mathbb{Z}^3, \mathbb{Z}^4$ são $\Delta = \frac{\pi}{4} \approx 0.785$, $\Delta = \frac{\pi}{6} \approx 0.524$ e $\Delta = \frac{\pi^2}{32} \approx 0.308$, respectivamente.
2. **Reticulado n -dimensional A_n :** Para todo $n \geq 1$, $A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1}; x_0 + x_1 + \dots + x_n = 0\}$ é um reticulado. Por definição, temos que A_n está contido no hiperplano $\sum_i x_i = 0$ no $\mathbb{R}^{n+1}$, possui uma matriz geradora B , dada por:

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & -1 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdots & -1 & 1 \end{bmatrix},$$

onde $\det A_n = \det(BB^t) = n + 1$, norma mínima igual a 2, raio de empacotamento $\rho = \frac{1}{\sqrt{2}}$ e densidade de centro $\delta = 2^{-n/2}(n + 1)^{-1/2}$.

3. **Reticulado hexagonal:** Temos que $A_1 \simeq \mathbb{Z}$ e que A_2 é equivalente ao reticulado hexagonal. O reticulado hexagonal é gerado pelos vetores $(1, 0)$ e $\left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right)$, e assim

sua matriz geradora é $B = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$. Desta forma $\det A_2 = \frac{3}{4}$, norma mínima igual a 1, raio de empacotamento $\rho = \frac{1}{2}$, densidade de empacotamento $\Delta = \frac{\pi}{\sqrt{12}} \approx 0,9069$ e densidade de centro $\delta = \frac{1}{\sqrt{12}}$.

4. **Reticulado D_n , para $n \geq 3$:** Temos que $D_n = \{(x_1, \dots, x_n) \in \mathbb{Z}^n : x_1 + \dots + x_n \text{ é par}\}$ é um reticulado. Sua matriz geradora é dada por;

$$B = \begin{bmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{bmatrix}$$

onde $\det D_n = 4$, norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$ e densidade de centro $\delta = 2^{-(n+2)/2}$.

5. Reticulado face-centered cubic: Temos que os reticulados A_3 e D_3 são equivalentes ao reticulado fcc . Assim, o fcc consiste de todos os pontos (x, y, z) , onde x, y, z são inteiros com soma par. Uma matriz geradora de D_3 é dada por;

$$B = \begin{bmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix},$$

onde $\det D_3 = 4$, norma mínima igual a 2, raio de empacotamento $\rho = 1/\sqrt{2}$, densidade $\Delta = \frac{\pi}{\sqrt{18}} \approx 0,7305$ e densidade de centro $\delta = 2^{-5/2}$.

- Para D_4 , temos $\Delta \approx 0,61685$ e densidade de centro $\delta \approx 0,125$.
- Para D_5 , temos $\Delta \approx 0,46526$ e densidade de centro $\delta \approx 0,08839$.

3.4 Homomorfismo canônico de um corpo de números

Para determinar o volume de uma família específica de reticulados e conseqüentemente, a densidade de centro é necessário falarmos das imersões de um corpo de números $\mathbb{K}$ no corpo dos números complexos $\mathbb{C}$.

Sejam $\mathbb{K}$ um corpo de números e n seu grau. Pelo Teorema 2.2.1 temos que existem n isomorfismos distintos $\sigma_j : \mathbb{K} \rightarrow \mathbb{C}$, uma vez que o polinômio minimal de um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{Q}$ tem somente n raízes em $\mathbb{C}$. Se $\sigma_j(\mathbb{K}) \subseteq \mathbb{R}$ diz-se que σ_j é **real**, caso

contrário σ_j é dito **imaginário**. Quando todos os monomorfismos são reais diz-se que $\mathbb{K}$ é um **corpo totalmente real** e quando os monomorfismos são todos imaginários diz-se que $\mathbb{K}$ é um **corpo totalmente imaginário**. Se $\alpha : \mathbb{C} \rightarrow \mathbb{C}$ é a conjugação complexa, então para todo $j = 1, \dots, n$, temos que $\alpha \circ \sigma_j = \sigma_k$, $1 \leq k \leq n$, e que $\sigma_j = \sigma_j$ se, e somente se, $\sigma_j(\mathbb{K}) \subset \mathbb{R}$. Assim, usando s para denotar o número de índices, tal que $\sigma_j(\mathbb{K}) \subset \mathbb{R}$, podemos ordenar os monomorfismos $\sigma_1, \dots, \sigma_n$ de tal modo que $\sigma_1, \dots, \sigma_s$ sejam os monomorfismos reais e $\sigma_{s+t+j} = \overline{\sigma_{s+j}}$; $j = 1, \dots, t$. Então $n - s$ é um número par, assim podemos escrever $s + 2t = n$. Daí, para cada $x \in \mathbb{K}$, temos que o homomorfismo $\sigma_{\mathbb{K}} : \mathbb{K} \rightarrow \mathbb{R}^n$ definido por

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \dots, \sigma_{s+t}(x)) \in \mathbb{R}^s \times \mathbb{R}^{2t},$$

é um homomorfismo injetivo de anéis, chamado de **homomorfismo canônico** de $\mathbb{K}$ em $\mathbb{R}^s \times \mathbb{R}^{2t}$. Geralmente identificamos $\mathbb{R}^s \times \mathbb{R}^{2t}$ com $\mathbb{R}^n$, e este homomorfismo pode também ser visto como

$$\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \dots, \sigma_s(x), \Re \sigma_{s+1}(x), \Im \sigma_{s+1}(x), \dots, \Re \sigma_{s+t}(x), \Im \sigma_{s+t}(x)),$$

onde as notações $\Re(x)$ e $\Im(x)$ representam as partes real e imaginária do número complexo x , respectivamente.

Exemplo 3.4.1 *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, $s = 0$ e $t = 1$. Para $x = a + bi \in \mathbb{K}$, $a, b \in \mathbb{Q}$, temos $\sigma_{\mathbb{K}}(x) = (R\sigma_1(x), I\sigma_1(x)) = (a, b)$.*

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

Proposição 3.4.1 *Seja $\mathbb{K}$ um corpo de números de grau n . Se M é um $\mathbb{Z}$ -módulo livre de $\mathbb{K}$ de posto n e se $(x_j)_{1 \leq j \leq n}$ é uma $\mathbb{Z}$ -base de M , então $\sigma_{\mathbb{K}}(M)$ é um reticulado no $\mathbb{R}^n$, com volume $\text{Vol}(\sigma_{\mathbb{K}}(M)) = 2^{-t} |\det_{1 \leq j, k \leq n}(\sigma_j(x_k))|$.*

Demonstração: Para cada j fixo, as coordenadas de $\sigma_{\mathbb{K}}(x_j)$ com respeito a base canônica do $\mathbb{R}^n$ são dadas por

$$(\sigma_1(x_j), \dots, \sigma_s(x_j), \Re \sigma_{s+1}(x_j), \Im \sigma_{s+1}(x_j), \dots, \Re \sigma_{s+t}(x_j), \Im \sigma_{s+t}(x_j)), \quad (3.4.3)$$

onde $\Re$ e $\Im$ denotam respectivamente, as partes real e imaginária. Agora calculemos o determinante D da matriz que tem a j -ésima coluna dada por (3.4.3), fazendo uso das seguintes fórmulas $\Re(z) = \frac{1}{2}(z + \bar{z})$, $\Im(z) = \frac{1}{2i}(z - \bar{z})$ para z em $\mathbb{C}$ e das transformações elementares no determinante, a saber, pela adição da $(s + 2l)$ -ésima linha a sua anterior e em seguida pela subtração da $(s + 2l - 1)$ -ésima coluna da sua posterior, para $l = 1, \dots, t$. Assim,

$$D = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_s(x_1) & \dots & \sigma_s(x_j) & \dots & \sigma_s(x_n) \\ \Re(\sigma_{s+1}(x_1)) & \dots & \Re(\sigma_{s+1}(x_j)) & \dots & \Re(\sigma_{s+1}(x_n)) \\ \Im(\sigma_{s+1}(x_1)) & \dots & \Im(\sigma_{s+1}(x_j)) & \dots & \Im(\sigma_{s+1}(x_n)) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \Re(\sigma_{s+t}(x_1)) & \dots & \Re(\sigma_{s+t}(x_j)) & \dots & \Re(\sigma_{s+t}(x_n)) \\ \Im(\sigma_{s+t}(x_1)) & \dots & \Im(\sigma_{s+t}(x_j)) & \dots & \Im(\sigma_{s+t}(x_n)) \end{vmatrix} =$$

$$\left(\frac{1}{2}\right)^{\frac{t}{2}} \left(\frac{1}{2i}\right)^{\frac{t}{2}} \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_s(x_1) & \dots & \sigma_s(x_j) & \dots & \sigma_s(x_n) \\ \sigma_{s+1}(x_1) + \overline{\sigma_{s+1}(x_1)} & \dots & \sigma_{s+1}(x_j) + \overline{\sigma_{s+1}(x_j)} & \dots & \sigma_{s+1}(x_n) + \overline{\sigma_{s+1}(x_n)} \\ \sigma_{s+1}(x_1) - \overline{\sigma_{s+1}(x_1)} & \dots & \sigma_{s+1}(x_j) - \overline{\sigma_{s+1}(x_j)} & \dots & \sigma_{s+1}(x_n) - \overline{\sigma_{s+1}(x_n)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_{s+t}(x_1) + \overline{\sigma_{s+t}(x_1)} & \dots & \sigma_{s+t}(x_j) + \overline{\sigma_{s+t}(x_j)} & \dots & \sigma_{s+t}(x_n) + \overline{\sigma_{s+t}(x_n)} \\ \sigma_{s+t}(x_1) - \overline{\sigma_{s+t}(x_1)} & \dots & \sigma_{s+t}(x_j) - \overline{\sigma_{s+t}(x_j)} & \dots & \sigma_{s+t}(x_n) - \overline{\sigma_{s+t}(x_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2}\right)^{\frac{t}{2}} \left(\frac{1}{2i}\right)^{\frac{t}{2}} 2^t \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_s(x_1) & \dots & \sigma_s(x_j) & \dots & \sigma_s(x_n) \\ \sigma_{s+1}(x_1) & \dots & \sigma_{s+1}(x_j) & \dots & \sigma_{s+1}(x_n) \\ \overline{\sigma_{s+1}(x_1)} & \dots & \overline{\sigma_{s+1}(x_j)} & \dots & \overline{\sigma_{s+1}(x_n)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_{s+t}(x_1) & \dots & \sigma_{s+t}(x_j) & \dots & \sigma_{s+t}(x_n) \\ \overline{\sigma_{s+t}(x_1)} & \dots & \overline{\sigma_{s+t}(x_j)} & \dots & \overline{\sigma_{s+t}(x_n)} \end{vmatrix} =$$

$$\left(\frac{1}{2i}\right)^t \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \sigma_2(x_1) & \dots & \sigma_2(x_j) & \dots & \sigma_2(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_s(x_1) & \dots & \sigma_s(x_j) & \dots & \sigma_s(x_n) \\ \sigma_{s+1}(x_1) & \dots & \sigma_{s+1}(x_j) & \dots & \sigma_{s+1}(x_n) \\ \sigma_{s+2}(x_1) & \dots & \sigma_{s+2}(x_j) & \dots & \sigma_{s+2}(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_{s+2t}(x_1) & \dots & \sigma_{s+2t}(x_j) & \dots & \sigma_{s+2t}(x_n) \end{vmatrix} = (2i)^{-t} \det(\sigma_j(x_k)).$$

Portanto, $D = (2i)^{-t} \det(\sigma_j(x_k))$, $j, k = 1, \dots, n$. Como $(x_j)_{1 \leq j \leq n}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$, segue da Proposição 2.4.3 que $\det(\sigma_j(x_k)) \neq 0$, e portanto, $D \neq 0$. Assim, os vetores $\sigma_{\mathbb{K}}(x_j)$ do $\mathbb{R}^n$ são linearmente independentes e geram $\sigma_{\mathbb{K}}(M)$, ou seja, $\sigma_{\mathbb{K}}(M)$ é um reticulado do $\mathbb{R}^n$. Do fato de $\{x_1, \dots, x_n\}$ ser uma $\mathbb{Z}$ -base de M , então $m = \sum_{j=1}^n a_j x_j$, $a_j \in \mathbb{Z}$, e portanto, $m \in M$. Assim, $\sigma_{\mathbb{K}}(m) = \sum_{j=1}^n a_j \sigma_{\mathbb{K}}(x_j)$, $a_j \in \mathbb{Z}$, ou seja, $\sigma_{\mathbb{K}}(M) = \left\{ \sum_{j=1}^n a_j \sigma_{\mathbb{K}}(x_j); a_j \in \mathbb{Z} \right\}$. Logo, $\text{Vol}(\sigma_{\mathbb{K}}(M)) = |D| = 2^t |\det_{1 \leq j, k \leq n}(\sigma_j(x_k))|$. $\blacksquare$

Exemplo 3.4.2 Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{3}]$ seu anel dos inteiros com $\mathbb{Z}$ -base $\{1, \sqrt{3}\}$. Como $\mathbb{K}$ é totalmente real, então $t = 0$, e portanto

$$\begin{vmatrix} \sigma_1(1) & \sigma_1(\sqrt{3}) \\ \sigma_2(1) & \sigma_2(\sqrt{3}) \end{vmatrix} = \begin{vmatrix} 1 & \sqrt{3} \\ 1 & -\sqrt{3} \end{vmatrix} = -2\sqrt{3}.$$

A imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{3}]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 em $\mathbb{R}^2$, cujo volume é $2\sqrt{3}$. $\blacksquare$

Exemplo 3.4.3 Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{6})$, e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{6}]$ seu anel dos inteiros com $\mathbb{Z}$ -base $\{1, \sqrt{6}\}$. Como $\mathbb{K}$ é totalmente real, então $t = 0$, e portanto

$$\text{Vol}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \left| \det \begin{pmatrix} 1 & \sqrt{6} \\ 1 & -\sqrt{6} \end{pmatrix} \right| = 2\sqrt{6}.$$

A imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{6}]) \subseteq \mathbb{R}^2$ é um reticulado de posto 2 em $\mathbb{R}^2$, cujo volume é $2\sqrt{6}$. $\blacksquare$

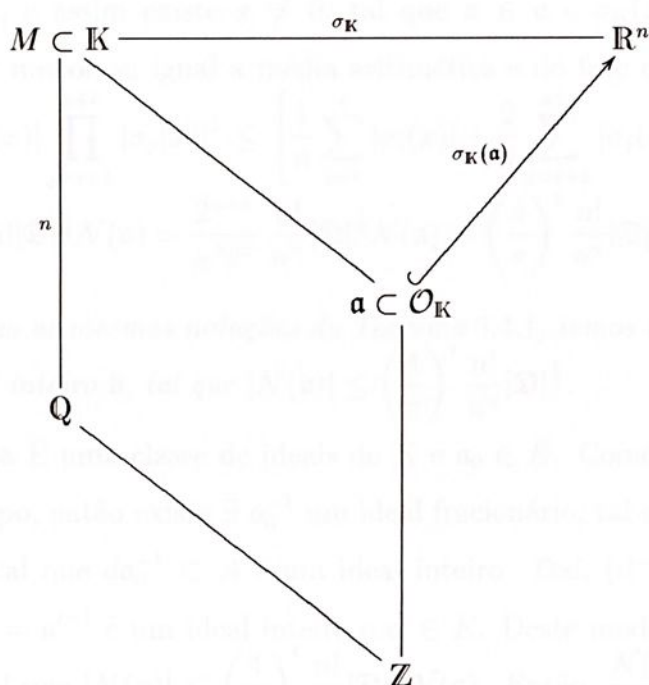
Exemplo 3.4.4 Tomemos $\mathbb{K} = \mathbb{Q}(\sqrt{-7})$, e $\mathcal{O}_{\mathbb{K}} = \mathbb{Z} \left[\frac{1 + \sqrt{-7}}{2} \right]$ seu anel dos inteiros com $\mathbb{Z}$ -base $\left\{ 1, \frac{1 + \sqrt{-7}}{2} \right\}$. Como $\mathbb{K}$ é totalmente imaginário, então $t = 1$, e portanto

$$\text{Vol}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{1}{2} \left| \det \begin{pmatrix} 1 & \frac{1 + \sqrt{-7}}{2} \\ 1 & \frac{1 - \sqrt{-7}}{2} \end{pmatrix} \right| = \frac{1}{2} \sqrt{7}.$$

Proposição 3.4.2 Seja $\mathbb{K}$ um corpo de números de grau n . Sejam $\mathfrak{D}$ o discriminante de $\mathbb{K}$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. Então, $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ e $\sigma_{\mathbb{K}}(\mathfrak{a})$ são reticulados, com respectivos volumes, $\text{Vol}(\mathcal{O}_{\mathbb{K}}) = 2^{-t} |\mathfrak{D}|^{\frac{1}{2}}$ e $\text{Vol}(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-t} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$, onde t é o número de monomorfismos imaginários.

Demonstração: Como $\mathfrak{a}$ e $\mathcal{O}_{\mathbb{K}}$ são $\mathbb{Z}$ -módulos livres de posto n , segue da Proposição 3.4.1 que $\sigma_{\mathbb{K}}(\mathfrak{a})$ e $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ são reticulados do $\mathbb{R}^n$ e que $\text{Vol}(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = 2^{-t} |\mathfrak{D}|$, onde $\{x_1, \dots, x_n\}$ é uma $\mathbb{Z}$ -base de $\mathcal{O}_{\mathbb{K}}$ e $\mathfrak{D} = \det(\sigma_i(x_k))^2$ (Proposição 2.4.3). Para a segunda fórmula, temos que $\sigma_{\mathbb{K}}(\mathfrak{a})$ é um subgrupo de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ de índice $\mathcal{N}(\mathfrak{a})$ uma vez que $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$ é isomorfo a $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})/\sigma_{\mathbb{K}}(\mathfrak{a})$. Além disso, como um domínio fundamental de $\sigma_{\mathbb{K}}(\mathfrak{a})$ é a união disjunta de $\mathcal{N}(\mathfrak{a})$ cópias de um domínio fundamental de $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$, segue que $\text{Vol}(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-t} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$, portanto $\text{Vol}(\mathcal{O}_{\mathbb{K}}) = 2^{-t} |\mathfrak{D}|^{\frac{1}{2}}$ e $\text{Vol}(\sigma_{\mathbb{K}}(\mathfrak{a})) = 2^{-t} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$. $\blacksquare$

A figura abaixo ilustra as Proposições 3.4.1 e 3.4.2.



Teorema 3.4.1 *Sejam K um corpo de números, n seu grau, s e t os inteiros como definidos anteriormente, $\mathfrak{D}$ o discriminante de K e $\mathfrak{a}$ um ideal não nulo inteiro de K . Então, $\mathfrak{a}$ possui um elemento não nulo x , tal que $|\mathcal{N}_Q^K(x)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$.*

Demonstração: Seja σ_K o homomorfismo canônico de K em $\mathbb{R}^s \times \mathbb{R}^{2t}$. Seja r um número real positivo e seja B_r o conjunto de todos os elementos $(y_1, \dots, y_s, z_1, \dots, z_t) \in \mathbb{R}^s \times \mathbb{R}^{2t}$, tal que $\sum_{i=1}^s |y_i| + 2 \sum_{j=1}^t |z_j| \leq r$. Então, B_r é um conjunto compacto, uma vez que é um conjunto fechado e limitado. Também é convexo, pois $\forall x, y \in B_r$, com $x = (y_1, \dots, y_s, z_1, \dots, z_t)$ e $y = (y'_1, \dots, y'_s, z'_1, \dots, z'_t)$, tem-se que $x, y \in B_r$, $\sum_{i=1}^s |y_i| + 2 \sum_{j=1}^t |z_j| \leq r$ e $\sum_{i=1}^s |y'_i| + 2 \sum_{j=1}^t |z'_j| \leq r$. Tomando α , tal que $0 \leq \alpha \leq 1$, temos que $\alpha x + (1 - \alpha)y \in B_r$ uma vez que $\sum_{i=1}^s |\alpha y_i + (1 - \alpha)y'_i| + 2 \sum_{j=1}^t |\alpha z_j + (1 - \alpha)z'_j| \leq \alpha \sum_{i=1}^s |y_i| + (1 - \alpha) \sum_{i=1}^s |y'_i| + 2\alpha \sum_{j=1}^t |z_j| + 2(1 - \alpha) \sum_{j=1}^t |z'_j| = \alpha \left(\sum_{i=1}^s |y_i| + 2 \sum_{j=1}^t |z_j| \right) + (1 - \alpha) \left(\sum_{i=1}^s |y'_i| + 2 \sum_{j=1}^t |z'_j| \right) \leq \alpha r + (1 - \alpha)r = r$. Assim, B_r é convexo. Além disso, temos que B_r é simétrico em relação a origem. Temos por [1][pg.66] que $\text{Vol}(B_r) = 2^s \left(\frac{\pi}{2}\right)^t \frac{r^n}{n!}$. Escolhemos r_0 , tal que $\text{Vol}(B_{r_0}) = 2^n (\sigma_K(\mathfrak{a}))$, ou seja,

$2^s \left(\frac{\pi}{2}\right)^t \frac{r_0^n}{n!} = 2^{n-t} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$, ou seja, $r_0^n = 2^{n-s} \pi^{-t} n! |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$. Pelo Teorema 3.1.6, segue que $B_r \cap \sigma_K(\mathfrak{a}) \neq \emptyset$, e assim existe $x \neq 0$, tal que $x \in \mathfrak{a}$ e $\sigma_K(x) \in B_r$. Do fato da média geométrica ser menor ou igual a média aritmética e do fato que $\sigma_K(x) \in B_r$, segue que $|\mathcal{N}(x)| = \prod_{i=1}^s |\sigma_i(x)| \prod_{j=s+1}^{s+t} |\sigma_j(x)|^2 \leq \left[\frac{1}{n} \sum_{i=1}^s |\sigma_i(x)| + \frac{2}{n} \sum_{j=s+1}^{s+t} |\sigma_j(x)| \right]^n \leq \frac{r_0^n}{n^n}$. Então, $|\mathcal{N}(x)| \leq \frac{1}{n^n} 2^{n-s} \pi^{-t} n! |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a}) = \frac{2^{n-s}}{\pi^{\frac{n-s}{2}}} \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a}) = \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$. $\blacksquare$

Corolário 3.4.1 *Com as mesmas notações do Teorema 3.4.1, temos que toda classe de ideal de $\mathbb{K}$ possui um ideal inteiro $\mathfrak{b}$, tal que $|\mathcal{N}(\mathfrak{b})| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}}$.*

Demonstração: Seja E uma classe de ideais de $\mathbb{K}$ e $\mathfrak{a}_0 \in E$. Como os ideais fracionários de A formam um grupo, então existe $\exists \mathfrak{a}_0^{-1}$ um ideal fracionário, tal que $\mathfrak{a}_0 \mathfrak{a}_0^{-1} = A$. Assim, existe $d \in A \setminus \{0\}$, tal que $d \mathfrak{a}_0^{-1} \subset A$ é um ideal inteiro. Daí, $(d^{-1} \mathfrak{a}_0)(d \mathfrak{a}_0^{-1}) = A$. Seja $\mathfrak{a}' = d^{-1} \mathfrak{a}_0$. Então, $\mathfrak{a} = \mathfrak{a}'^{-1}$ é um ideal inteiro e $\mathfrak{a}' \in E$. Deste modo, pelo Teorema 3.4.1, existe $x \in \mathfrak{a} \setminus \{0\}$, tal que $|\mathcal{N}(x)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}} \mathcal{N}(\mathfrak{a})$. Então, $\frac{\mathcal{N}(Ax)}{\mathcal{N}(\mathfrak{a})} \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}}$. Como $\mathcal{N}(Ax) = \mathcal{N}(Ax \mathfrak{a}^{-1} \mathfrak{a}) = \mathcal{N}(Ax \mathfrak{a}^{-1}) \mathcal{N}(\mathfrak{a})$, segue que $\frac{\mathcal{N}(Ax)}{\mathcal{N}(\mathfrak{a})} = \mathcal{N}(Ax \mathfrak{a}^{-1})$. Temos que $Ax \mathfrak{a}^{-1} = Ax \mathfrak{a}'$ é um ideal inteiro, pois é um produto de um ideal principal por $\mathfrak{a}'$. Temos também que $Ax \subset \mathfrak{a} \iff \mathfrak{a} \mid Ax \iff \exists \mathfrak{b}$ ideal inteiro, tal que $Ax = \mathfrak{a} \mathfrak{b} \iff Ax \mathfrak{a}^{-1} = \mathfrak{b}$. Portanto, existe $\mathfrak{b}$ ideal inteiro, tal que $|\mathcal{N}(\mathfrak{b})| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}}$. $\blacksquare$

Corolário 3.4.2 *Com as mesmas notações do Teorema 3.4.1, temos que $|\mathfrak{D}| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$, para $n \geq 2$ e $\frac{n}{\log|\mathfrak{D}|}$ é limitado por uma constante independente de $\mathbb{K}$.*

Demonstração: Pelo Corolário 3.4.1, existe um ideal inteiro não nulo $\mathfrak{b}$ em $\mathbb{K}$, tal que $1 \leq \mathcal{N}(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |\mathfrak{D}|^{\frac{1}{2}}$, ou seja, $|\mathfrak{D}|^{\frac{1}{2}} \geq \left(\frac{\pi}{4}\right)^t \frac{n^n}{n!}$. Portanto, $|\mathfrak{D}| \geq \left(\frac{\pi}{4}\right)^{2t} \frac{n^{2n}}{(n!)^2}$. Seja $a_n = \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{n!^2}$. Então, $a_1 = \frac{\pi}{4}$, $a_2 = \left(\frac{\pi}{4}\right)^2 \frac{2^4 \pi^2}{2^2 4} = \frac{\pi}{4}$, e que $\frac{a_{n+1}}{a_n} = \frac{\pi}{4} \frac{(n+1)^{2(n+1)}}{((n+1)!)^2} \frac{n!^2}{n^{2n}} = \frac{\pi}{4} \frac{(n+1)^{2n}}{n^{2n}} = \frac{\pi}{4} \left(\frac{n+1}{n}\right)^{2n} = \frac{\pi}{4} \left(1 + \frac{1}{n}\right)^{2n} = \frac{\pi}{4} (1 + 2 + \text{termos positivos}) \geq \frac{3\pi}{4}$. Assim, $\frac{a_{n+1}}{a_n} \geq \frac{3\pi}{4}$ e $a_n = \frac{a_n}{a_{n-1}} \frac{a_{n-1}}{a_{n-2}} \dots \frac{a_3}{a_2} a_2 \geq \left(\frac{3\pi}{4}\right)^{n-2} \frac{\pi^2}{4} = \left(\frac{3\pi}{4}\right)^{n-2} \frac{3\pi}{4} \frac{\pi}{3} = \left(\frac{3\pi}{4}\right)^{n-1} \frac{\pi}{3}$. Como, $\left(\frac{\pi}{4}\right)^{2t} \frac{n^{2n}}{(n!)^2} < \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2}$ e $|\mathfrak{D}| \geq \left(\frac{\pi}{4}\right)^{2t} \frac{n^{2n}}{(n!)^2}$, segue que, $|\mathfrak{D}| \geq \left(\frac{\pi}{4}\right)^n \frac{n^{2n}}{(n!)^2} \geq$

$\left(\frac{3\pi}{4}\right)^{n-1} \frac{\pi}{3}$. Agora, temos que $|\mathfrak{D}| \geq \left(\frac{3\pi}{4}\right)^n \frac{4}{3\pi} \frac{\pi}{3} = \left(\frac{3\pi}{4}\right)^n \frac{4}{9}$. Como $\frac{4}{9} = \left(\frac{2}{3}\right)^2 \geq \left(\frac{2}{3}\right)^n$, segue que $|\mathfrak{D}| \geq \left(\frac{3\pi}{4}\right)^n \left(\frac{2}{3}\right)^n = \left(\frac{\pi}{2}\right)^n$. Portanto, $\log|\mathfrak{D}| = n \log \frac{\pi}{2}$, ou seja, $\frac{n}{\log|\mathfrak{D}|} \leq \frac{1}{\log \frac{\pi}{2}}$. $\blacksquare$

Proposição 3.4.3 *Sejam $\mathbb{K}$ um corpo de números e $x \in \mathbb{K}$. Então, $|\sigma_{\mathbb{K}}(x)|^2 = c \cdot \text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x})$, onde*

$$c = \begin{cases} 1 & \text{se } \mathbb{K} \text{ for totalmente real,} \\ \frac{1}{2} & \text{se } \mathbb{K} \text{ for totalmente imaginário.} \end{cases}$$

Demonstração: Se $\mathbb{K}$ for totalmente real, temos que $\sigma_{\mathbb{K}}(x) = (\sigma_1(x), \dots, \sigma_n(x))$, para $x \in \mathbb{K}$. Assim, $|\sigma_{\mathbb{K}}(x)|^2 = \sigma_1(x)^2 + \dots + \sigma_n(x)^2 = \sigma_1(x^2) + \dots + \sigma_n(x^2) = \sigma_1(x\bar{x}) + \dots + \sigma_n(x\bar{x}) = \text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x})$.

Se $\mathbb{K}$ é totalmente imaginário, temos $\sigma_{\mathbb{K}}(x) = (\Re\sigma_1(x), \Im\sigma_1(x), \dots, \Re\sigma_{\frac{n}{2}}(x), \Im\sigma_{\frac{n}{2}}(x))$, para $x \in \mathbb{K}$ e $|\sigma_{\mathbb{K}}(x)|^2 = (\Re\sigma_1(x))^2 + (\Im\sigma_1(x))^2 + \dots + (\Re\sigma_{\frac{n}{2}}(x))^2 + (\Im\sigma_{\frac{n}{2}}(x))^2 = \sigma_1(x)\bar{\sigma}_1(x) + \dots + \sigma_{\frac{n}{2}}(x)\bar{\sigma}_{\frac{n}{2}}(x) = \sigma_1(x)\sigma_1(\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x)\sigma_{\frac{n}{2}}(\bar{x}) = \sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x})$. Por outro lado, $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x}) + \bar{\sigma}_1(x\bar{x}) + \dots + \bar{\sigma}_{\frac{n}{2}}(x\bar{x})$. Visto que $\bar{\sigma}_1(x\bar{x}) = \sigma_1(x\bar{x})$, temos que $\text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x}) = 2(\sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x}))$, e assim $\frac{1}{2}\text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \dots + \sigma_{\frac{n}{2}}(x\bar{x})$. Portanto, $|\sigma_{\mathbb{K}}(x)|^2 = \frac{1}{2} \cdot \text{Tr}_{\mathbb{K}/\mathbb{Q}}(x\bar{x})$. $\blacksquare$

Observação 3.4.1 *Fazendo $t_{\mathfrak{a}} = \min\{\text{Tr}(x\bar{x}); x \neq 0, x \in \mathfrak{a}\}$ para um corpo de número $\mathbb{K}$,*

$$\text{então } \delta(\sigma_{\mathbb{K}}(\mathfrak{a})) = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)^{\frac{n}{2}}}{|\mathfrak{D}_{\mathbb{K}}|^{\frac{1}{2}} \cdot \mathcal{N}(\mathfrak{a})}$$

Teorema 3.4.2 (Hermite) *Todo corpo numérico $\mathbb{K} \neq \mathbb{Q}$, tem discriminante $\mathfrak{D} \neq \pm 1$.*

Demonstração: Pelo Corolário 3.4.2, temos que $|\mathfrak{D}| \geq \left(\frac{3\pi}{4}\right)^{n-1} \frac{\pi}{3}$. Como $\frac{3\pi}{4} > 1$ e $\frac{\pi}{3} > 1$, segue que, $|\mathfrak{D}| > 1$, ou seja, $\mathfrak{D} \neq \pm 1$. $\blacksquare$

Capítulo 4

Aplicações no $\mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^4$ e $\mathbb{R}^5$

Este Capítulo tem por objetivo a aplicação dos resultados apresentados nos capítulos anteriores, mais precisamente, calcular a densidade de centro dos reticulados obtidos via o homomorfismo canônico. Nosso maior desafio no cálculo efetivo da densidade de centro é minimizar uma forma quadrática, caracterizada em função do traço relativo. No caso dos corpos quadráticos caracterizamos a forma quadrática e calculamos a densidade de centro da realização geométrica (imagem de um ideal via o homomorfismo canônico) do anel dos inteiros algébricos e de ideais principais. No estudo das cúbicas, quárticas e quárticas, restringimo-nos à aquelas da forma $\mathbb{Q}(\sqrt[3]{d})$, $\mathbb{Q}(\sqrt[4]{d})$ e $\mathbb{Q}(\sqrt[5]{d})$, com d um inteiro livre de quadrados. Sob tais condições caracterizamos o anel dos inteiros algébricos e sua forma quadrática. O valor mínimo da forma quadrática é obtido atribuindo valores inteiros às variáveis e comparando os resultados. No caso de um ideal do anel dos inteiros algébricos de $\mathbb{Q}(\sqrt[3]{d})$, $\mathbb{Q}(\sqrt[4]{d})$ e $\mathbb{Q}(\sqrt[5]{d})$ a forma quadrática é minimizada com valores inteiros e ainda satisfazendo condições que caracterizam os elementos do ideal.

O Lema de Kummer 2.9.3 é de fundamental importância neste contexto. Com este resultado podemos descrever os geradores de ideais primos e obter o grau residual e o índice de ramificação.



4.1 Reticulados em corpos quadráticos

Nesta seção temos o objetivo de calcular a densidade de centro de reticulados de posto 2 em $\mathbb{R}^2$. Pela Proposição 2.2.1 temos que todo corpo quadrático tem a forma $K = \mathbb{Q}(\sqrt{d})$, com d um número inteiro livre de quadrados e que seu anel de inteiros algébricos é $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ se d é congruente a 2 ou 3 módulo 4, com $\mathfrak{D}_K = 4d$ ou $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ se d é congruente a 1 módulo 4 com $\mathfrak{D}_K = d$. Sejam $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$ e $t_{\mathfrak{a}} = \min\{Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}); \alpha \in \mathfrak{a}, \alpha \neq 0\}$. Assim, no caso em que o ideal é o próprio anel, temos pela Observação 3.4.1 que a densidade de centro do reticulado $\sigma_K(\mathcal{O}_K)$ é dada por $\delta(\sigma_K(\mathcal{O}_K)) = \frac{\left(\frac{t_{\mathcal{O}_K}}{4}\right)}{|\mathfrak{D}_K|^{\frac{1}{2}}}$.

Exemplo 4.1.1 Sejam $K = \mathbb{Q}(\sqrt{7})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{7}]$ e $\mathfrak{D}_K = 28$. Dado $\alpha = a + b\sqrt{7} \in \mathcal{O}_K$, temos que $\alpha\bar{\alpha} = (a + b\sqrt{7})(a + b\sqrt{7}) = a^2 + 2ab\sqrt{7} + 7b^2$. Assim, $Tr(\alpha\bar{\alpha}) = Tr(a^2 + 2ab\sqrt{7} + 7b^2) = Tr(a^2) + Tr(2ab\sqrt{7}) + Tr(7b^2) = 2a^2 + 14b^2 = 2(a^2 + 7b^2)$, e daí $t_{\mathcal{O}_K} = \min\{Tr(\alpha\bar{\alpha}); \alpha \neq 0, \alpha \in \mathcal{O}_K\} = 2$, para $a = 1$ e $b = 0$. Portanto, $\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{2\sqrt{28}} \simeq 0,09449$. ■

Exemplo 4.1.2 Sejam $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ e $\mathfrak{D}_K = 5$. Dado $\alpha = a + b\sqrt{5} \in \mathcal{O}_K$, temos que $\alpha\bar{\alpha} = (a + b\sqrt{5})(a + b\sqrt{5}) = a^2 + 2ab\sqrt{5} + 5b^2$. Assim, $Tr(\alpha\bar{\alpha}) = Tr(a^2 + 2ab\sqrt{5} + 5b^2) = Tr(a^2) + Tr(2ab\sqrt{5}) + Tr(5b^2) = 2a^2 + 10b^2 = 2(a^2 + 5b^2)$, e daí $t_{\mathcal{O}_K} = \min\{Tr(\alpha\bar{\alpha}); \alpha \neq 0, \alpha \in \mathcal{O}_K\} = 2$, para $a = 1$ e $b = 0$. Portanto, $\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{2\sqrt{5}} \simeq 0,2236$. ■

Consideremos agora ideais principais do anel dos inteiros algébricos de um corpo quadrático K . Seja $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$, tal que $\mathfrak{a} = \gamma\mathcal{O}_K$, onde $\gamma \in \mathcal{O}_K$. Então, $\sigma_K(\mathfrak{a})$ é um reticulado de posto 2 no $\mathbb{R}^2$ e sua densidade de centro, pela Observação 3.4.1, é dada por;

$$\delta(\sigma_K(\mathfrak{a})) = \frac{\left(\frac{t_{\mathfrak{a}}}{4}\right)}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot |\mathcal{N}(\gamma)|}.$$

Exemplo 4.1.3 Sejam $K = \mathbb{Q}(\sqrt{11})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{11}]$ e $\mathfrak{a}$ o ideal principal de $\mathcal{O}_K$, gerado por $\gamma = 1 + 2\sqrt{11}$. Dado $\alpha \in \gamma\mathcal{O}_K$, existem $a, b \in \mathbb{Z}$, tais que $\alpha = (a + 22b) + (2a + b)\sqrt{11}$, onde $\alpha\bar{\alpha} = (a + 22b)^2 + 11(2a + b)^2 + 2(a + 22b)(2a + b)\sqrt{11}$ e $Tr(\alpha\bar{\alpha}) = 2[(a + 22b)^2 + 11(2a + b)^2]$, assim $t_{\mathfrak{a}} = \min\{Tr(\alpha\bar{\alpha}); \alpha \neq 0, \alpha \in \mathcal{O}_K\} = 90$, para $a = 1$ e $b = 0$. Como $\mathfrak{D}_K = 44$ e $\mathcal{N}(\langle 1 + 2\sqrt{11} \rangle) = |\mathcal{N}(1 + 2\sqrt{11})| = |-43| = 43$, temos $\delta(\sigma_K(\mathfrak{a})) = \frac{45}{172\sqrt{11}} \simeq 0,0788$. ■

Exemplo 4.1.4 Sejam $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ e $\mathfrak{a}$ o ideal principal de $\mathcal{O}_K$, gerado por $\gamma = 7 + 2\sqrt{5}$. Dado $\alpha \in \gamma\mathcal{O}_K$, existem $a, b \in \mathbb{Z}$, tais que $\alpha = \left(a + \frac{b}{2}\right) + \frac{b\sqrt{5}}{2}(7 + \sqrt{5}) = \left(7a + \frac{17b}{2}\right) + \left(2a + \frac{9b}{2}\right)\sqrt{5}$, onde $\alpha\bar{\alpha} = \left(7a + \frac{17b}{2}\right)^2 + 5\left(2a + \frac{9b}{2}\right)^2 + 2\left(7a + \frac{17b}{2}\right)\left(2a + \frac{9b}{2}\right)\sqrt{5}$ e $Tr(\alpha\bar{\alpha}) = 2\left[\left(7a + \frac{17b}{2}\right)^2 + 5\left(2a + \frac{9b}{2}\right)^2\right]$. Assim, $t_{\mathfrak{a}} = \min\{Tr(\alpha\bar{\alpha}); \alpha \neq 0, \alpha \in \mathfrak{a}\} = 138$, para $a = 1$ e $b = 0$. Como $\mathfrak{D}_K = 5$ e como $\mathcal{N}(\langle 7 + 2\sqrt{5} \rangle) = |\mathcal{N}(7 + 2\sqrt{5})| = |29| = 29$, temos que a densidade de centro do reticulado $\sigma_K(\mathfrak{a})$ é $\delta(\sigma_K(\mathfrak{a})) = \frac{69}{58\sqrt{5}} \simeq 0,5320$. $\blacksquare$

Proposição 4.1.1 Quando K é um corpo quadrático totalmente imaginário e $\mathfrak{a}$ é um ideal principal do anel dos inteiros algébricos de K , a densidade de centro do reticulado $\sigma_K(\mathfrak{a})$ é a mesma do reticulado $\sigma_K(\mathcal{O}_K)$.

Demonstração: Sejam $\mathfrak{a} = \gamma\mathcal{O}_K$ um ideal principal de $\mathcal{O}_K$ e $x \in \mathfrak{a}$, onde $x = \gamma l$, com $l \in \mathcal{O}_K$. Assim, $x\bar{x} = \gamma\bar{\gamma}l\bar{l}$ e $Tr_{K/\mathbb{Q}}(\gamma\bar{\gamma}l\bar{l}) = 2(\gamma\bar{\gamma}l\bar{l})$. Como

$$\frac{\sqrt{\frac{1}{2}Tr_{K/\mathbb{Q}}(\gamma\bar{\gamma}l\bar{l})}}{2} = \sqrt{\gamma\bar{\gamma}} \cdot \frac{\sqrt{l\bar{l}}}{2},$$

segue que, $\rho_{\gamma\mathcal{O}_K} = |\mathcal{N}(\gamma)| \cdot \rho_{\mathcal{O}_K}$, e portanto,

$$\delta(\sigma_K(\gamma\mathcal{O}_K)) = \frac{2\rho_{\gamma\mathcal{O}_K}^2}{|\mathcal{D}_K|^{\frac{1}{2}} \cdot |\mathcal{N}(\gamma)|} = \frac{2\rho_{\mathcal{O}_K}^2}{|\mathcal{D}_K|^{\frac{1}{2}}} = \delta(\sigma_K(\mathcal{O}_K)).$$

Exemplo 4.1.5 Sejam $K = \mathbb{Q}(\sqrt{-7})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$ e $\alpha = a + b\omega \in \mathcal{O}_K$, com $\omega = \frac{11 + \sqrt{-7}}{2}$. Então, $\alpha\bar{\alpha} = a^2 + ab\bar{\omega} + ab\omega$ e $Tr(\alpha\bar{\alpha}) = 2(a^2 + ab + 2b^2)$. Assim, segue que $t_{\mathcal{O}_K} = \min\{Tr(\alpha\bar{\alpha}); \alpha \neq 0, \alpha \in \mathcal{O}_K\} = 2$, para $a = 1$ e $b = 0$. Visto que $\mathfrak{D}_K = -7$, temos que a densidade de centro do reticulado $\sigma_K(\mathcal{O}_K)$ é $\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{2\sqrt{7}} \simeq 0,1889$. $\blacksquare$

Exemplo 4.1.6 Sejam $K = \mathbb{Q}(\sqrt{-2})$, $\mathcal{O}_K = \mathbb{Z}[\omega]$ e $\alpha = a + b\omega \in \mathcal{O}_K$, com $\omega = \sqrt{-2}$. Então, $\alpha\bar{\alpha} = a^2 + 7b^2\omega$ e $Tr(\alpha\bar{\alpha}) = 2(a^2 + 7b^2)$. Assim, $t_{\mathcal{O}_K} = \min\{Tr(\alpha\bar{\alpha}); \alpha \neq 0, \alpha \in \mathcal{O}_K\} = 2$, para $a = 1$ e $b = 0$. Visto que $\mathfrak{D}_K = -8$, temos que a densidade de centro do reticulado $\sigma_K(\mathcal{O}_K)$ é $\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{4\sqrt{2}} \simeq 0,3535$. $\blacksquare$

4.2 Reticulados nas Cúbicas

Nesta seção faremos o estudo de casos particulares de cúbicas, com o objetivo de obter reticulados de posto 3 no $\mathbb{R}^3$. Aqui descreveremos o anel dos inteiros algébricos de $K = \mathbb{Q}(\sqrt[3]{d})$, o discriminante de K , a forma quadrática associada e os reticulados obtidos em $\mathbb{R}^3$ a partir dos ideais ordinários de $\mathcal{O}_K$.

Teorema 4.2.1 [6] *Sejam d um inteiro livre de quadrados, $\theta = \sqrt[3]{d}$, $K = \mathbb{Q}(\theta)$, $\omega = \frac{1+\theta+\theta^2}{3}$ e $\gamma = \frac{1-\theta+\theta^2}{3}$. Então, o anel $\mathcal{O}_K$ dos inteiros algébricos de K é dado por:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\theta] & \text{se } d \not\equiv \pm 1 \pmod{9} \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\omega & \text{se } d \equiv 1 \pmod{9} \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\gamma & \text{se } d \equiv -1 \pmod{9}. \end{cases}$$

Sobre as mesmas condições do Teorema 4.2.1, dado $\alpha \in K$, $\alpha = a_0 + a_1\theta + a_2\theta^2$ e visto que o número de monomorfismo imaginário é um, ou seja, $t = 1$, o homomorfismo canônico σ_K de K em $\mathbb{R}^3$ é dado por $\sigma_K(\alpha) = (\alpha, \Re\sigma_2(\alpha), \Im\sigma_2(\alpha))$, e portanto,

$$\begin{aligned} |\sigma_K(\alpha)|^2 &= \alpha^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = \alpha^2 + \sigma_2(\alpha)\sigma_2(\bar{\alpha}) \\ &= (a_0 + a_1\theta + a_2\theta^2) + (a_0 + a_1\theta\xi + a_2\theta^2\xi^2)(a_0 + a_1\theta\xi + a_2\theta^2\xi^2) \\ &= 2a_0^2 + 2a_1^2\theta^2 + 2a_2^2\theta^4 + a_0a_1\theta + a_1a_2d + a_0a_2\theta^2 \\ &= 2a_0^2 + 2(a_1\theta)^2 + 2(a_2\theta^2)^2 + a_0(a_1\theta) + (a_1\theta)(a_2\theta^2) + a_0(a_2\theta^2). \end{aligned}$$

Esta forma quadrática é minimizada em $a = 1$, $b = c = 0$, e assumindo o valor 2. Desta forma, $\rho = \frac{\sqrt{2}}{2}$. Dado que $\mathfrak{D}_K = \pm\mathcal{N}(f'(\theta)) = \pm 27d^2$, temos que a densidade de centro do reticulado $\sigma_K(\mathcal{O}_K)$ é dado por $\delta(\sigma_K(\mathcal{O}_K)) = \frac{2(\sqrt{2}/2)^3}{\sqrt{27d^2}} = \frac{1}{3\sqrt{6}d}$.

Exemplo 4.2.1 *Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{3}$, $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{3}]$ o anel dos inteiros algébricos de K e $X^3 - 3$ o polinômio irredutível de $\sqrt[3]{3}$ sobre $\mathbb{Q}$. Consideremos o ideal $2\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^3 - 3$ fatora-se como:*

$$X^3 - 3 \equiv (X - 1)(X^2 + X + 1) \pmod{2\mathbb{Z}[X]}.$$

Pelo Lema de Kummer, temos que $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, tal que $\mathfrak{p}_1 = (2, \theta - 1)$ e $\mathfrak{p}_2 = (2, \theta^2 + \theta + 1)$, sendo esses os ideais primos acima de $2\mathbb{Z}$, cujo os graus residuais são 1 e as normas são 2 e

4, respectivamente. Além disso, $\mathcal{D}_K = \pm 27 \cdot 9$. Desta forma para calcularmos a densidade de centro do ideal primo $\sigma_K(\mathfrak{p}_1)$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, temos que $\alpha = a_0 + a_1\theta + a_2\theta^2$ e como $\mathfrak{p}_1$ está acima de $2\mathbb{Z}$ e $\theta \equiv 1 \pmod{\mathfrak{p}_1}$, então $\alpha \in \mathfrak{p}_1$ se, e somente se, $a_0 + a_1 + a_2 \in 2\mathbb{Z}$. Daí nosso próximo passo é minimizar a forma quadrática.

$$|\sigma_K(\alpha)|^2 = 2a_0^2 + 2(a_1\theta)^2 + 2(a_2\theta^2)^2 + a_0(a_1\theta) + (a_1\theta)(a_2\theta^2) + a_0(a_2\theta^2),$$

para valores de $a_0, a_1, a_2 \in \mathbb{Z}$ que satisfazem a condição $a_0 + a_1 + a_2 \in 2\mathbb{Z}$. Analisando todas as possibilidades, temos que a forma quadrática $|\sigma_K(\alpha)|^2$ assume o menor valor quando $a_0 = a_1 = 1, a_2 = 0$, e este valor é $2\theta^2 + \theta + 2$, logo

$$\rho = \frac{\sqrt{2\theta^2 + \theta + 2}}{2} \quad e \quad \delta(\sigma_K(\mathfrak{p}_1)) = \frac{2 \left(\frac{\sqrt{2\theta^2 + \theta + 2}}{2} \right)^3}{\sqrt{27 \cdot 9 \cdot 2}} = \frac{(\sqrt{2\theta^2 + \theta + 2})^3}{72\sqrt{3}} \approx 0,1680. \quad \blacksquare$$

Exemplo 4.2.2 Sejam $K = \mathbb{Q}(\theta), \theta = \sqrt[3]{3}, \mathcal{O}_K = \mathbb{Z}[\sqrt[3]{3}]$ o anel dos inteiros algébricos de K e $X^3 - 3$ o polinômio irredutível de $\sqrt[3]{3}$ sobre $\mathbb{Q}$. Consideremos o ideal $5\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^3 - 3$ fatora-se como:

$$X^3 - 3 \equiv (X - 2)(X^2 + 2X - 1) \pmod{5\mathbb{Z}[X]}.$$

Pelo Lema de Kummer, temos que $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, tal que $\mathfrak{p}_1 = (5, \theta - 2)$ e $\mathfrak{p}_2 = (5, \theta^2 + 2\theta - 1)$, sendo esses os ideais primos acima de $5\mathbb{Z}$, cujo os graus residuais são 1 e as normas são 3 e 9, respectivamente. Além disso, $\mathcal{D}_K = \pm 27 \cdot 9$. Desta forma para calcularmos a densidade de centro do ideal primo $\sigma_K(\mathfrak{p}_1)$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, temos que $\alpha = a_0 + a_1\theta + a_2\theta^2$ e como $\mathfrak{p}_1$ está acima de $5\mathbb{Z}$ e $\theta \equiv 2 \pmod{\mathfrak{p}_1}$, então $\alpha \in \mathfrak{p}_1$ se, e somente se, $a_0 + 2a_1 - a_2 \in 5\mathbb{Z}$. Daí nosso próximo passo é minimizar a forma quadrática.

$$|\sigma_K(\alpha)|^2 = 2a_0^2 + 2(a_1\theta)^2 + 2(a_2\theta^2)^2 + a_0(a_1\theta) + (a_1\theta)(a_2\theta^2) + a_0(a_2\theta^2),$$

para valores de $a_0, a_1, a_2 \in \mathbb{Z}$ que satisfazem a condição $a_0 + 2a_1 - a_2 \in 5\mathbb{Z}$. Analisando todas as possibilidades, temos que a forma quadrática $|\sigma_K(\alpha)|^2$ assume o menor valor quando $a_0 = 1, a_1 = 2$ e $a_2 = 0$, e este valor é $2 + 2\theta + 8\theta^2$, logo

$$\rho = \frac{\sqrt{2 + 2\theta + 8\theta^2}}{2} \quad e \quad \delta(\sigma_K(\mathfrak{p}_1)) = \frac{2 \left(\frac{\sqrt{2 + 2\theta + 8\theta^2}}{2} \right)^3}{\sqrt{27 \cdot 9 \cdot 3}} \approx 0,1271. \quad \blacksquare$$

Exemplo 4.2.3 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$, $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ o anel dos inteiros algébricos de K e $X^3 - 2$ o polinômio irredutível de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Consideremos o ideal $3\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^3 - 2$ fatora-se como:

$$X^3 - 2 \equiv (X + 1)^3 \pmod{3\mathbb{Z}[X]}.$$

Pelo Lema de Kummer, temos que $3\mathcal{O}_K = \mathfrak{p}^3$, tal que $\mathfrak{p} = (3, \theta + 1)$ sendo o único ideal primo acima de $3\mathbb{Z}$, cujo o grau residual é 1 e a norma é 3. Além disso, $t = 1$ e $\mathfrak{D}_K = \pm 27 \cdot 4$. Desta forma para calcularmos a densidade de centro do ideal primo $\sigma_K(\mathfrak{p})$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, temos que $\alpha = a_0 + a_1\theta + a_2\theta^2$ e como $\mathfrak{p}$ esta acima de $3\mathbb{Z}$ e $\theta \equiv -1 \pmod{\mathfrak{p}}$, então $\alpha \in \mathfrak{p}$ se, e somente se, $a_0 - a_1 + a_2 \in 3\mathbb{Z}$. Daí nosso próximo passo é minimizar a forma quadrática.

$$|\sigma_K(\alpha)|^2 = 2a_0^2 + 2(a_1\theta)^2 + 2(a_2\theta^2)^2 + a_0(a_1\theta) + (a_1\theta)(a_2\theta^2) + a_0(a_2\theta^2),$$

para valores de $a_0, a_1, a_2 \in \mathbb{Z}$ que satisfazem a condição $a_0 - a_1 + a_2 \in 3\mathbb{Z}$. Analisando todas as possibilidades, temos que a forma quadrática $|\sigma_K(\alpha)|^2$ assume o menor valor quando $a_0 = 1, a_1 = 0$ e $a_2 = -1$, e este valor é $2 + 4\theta - \theta^2$ logo,

$$\rho = \frac{\sqrt{2 + 4\theta - \theta^2}}{2} \text{ e } \delta(\sigma_K(\mathfrak{p})) = \frac{2 \left(\frac{\sqrt{2 + 4\theta - \theta^2}}{2} \right)^3}{\sqrt{27 \cdot 4 \cdot 3}} \approx 0,1021. \quad \blacksquare$$

4.3 Reticulados nas Quárticas

Nesta seção faremos o estudo de casos particulares de quárticas, com o objetivo de obter reticulados de posto 4 no $\mathbb{R}^4$. Aqui descreveremos o anel dos inteiros algébricos de $K = \mathbb{Q}(\sqrt[4]{d})$, com d um inteiro livre de quadrados, o discriminante de K , a forma quadrática associada e a descrição dos reticulados obtidos em $\mathbb{R}^4$ a partir dos ideais ordinários de $\mathcal{O}_K$.

Teorema 4.3.1 [4] Sejam d um inteiro livre de quadrados, $\theta = \sqrt[4]{d}$, $K = \mathbb{Q}(\theta)$, $\omega = \frac{1 + \theta^2}{2}$ e $\gamma = \frac{\theta + \theta^3}{2}$. Então, o anel $\mathcal{O}_K$ dos inteiros algébricos de K é dado por:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\theta] & \text{se } d \not\equiv 1 \pmod{4} \\ \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\omega + \mathbb{Z}\gamma & \text{se } d \equiv 1 \pmod{4}. \end{cases}$$

Sobre as mesmas condições do Teorema 4.3.1, dado $\alpha \in \mathbb{K}$, existem $a_0, a_1, a_2, a_3 \in \mathbb{Z}$, tal que $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$ se $t = 1$, então o homomorfismo canônico $\sigma_{\mathbb{K}}$ de $\mathbb{K}$ em $\mathbb{R}^4$ é dado por $\sigma_{\mathbb{K}}(\alpha) = (\alpha_1, \alpha_2, \Re\sigma_3(\alpha), \Im\sigma_3(\alpha))$, e portanto,

$$\begin{aligned} |\sigma_{\mathbb{K}}(\alpha)|^2 &= \alpha_1^2 + \alpha_2^2 + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} = 3a_0^2 + 2a_0a_2\theta^2 + 3a_1^2\theta^2 + 2a_1a_3\theta^4 + 3a_2^2\theta^4 + 3a_3^2\theta^6 \\ &= 3a_0^2 + 2a_0(a_2\theta^2) + 3(a_1\theta)^2 + 2a_1\theta(a_3\theta^3) + 3(a_2\theta)^2 + 3(a_3\theta^3)^2 \\ &= \frac{1}{2}\{2a_0^2 + 2a_1\theta^2 + 5a_2^2\theta^4 + 5a_3^2\theta^4 + (2a_0 + a_2\theta^2)^2 + (2a_1\theta + a_3\theta^3)^2\}. \end{aligned}$$

Esta forma quadrática é minimizada em $a_0 = 1, a_1 = a_2 = a_3 = 0$, e assumindo o valor 3. Desta forma, $\rho = \frac{\sqrt{3}}{2}$. Dado que $\mathfrak{D}_{\mathbb{K}} = \pm\mathcal{N}(f'(\theta)) = \pm 256d^3$, temos que a densidade de centro do reticulado $\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})$ é dada por $\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{2^t \rho^n}{\mathfrak{D}_{\mathbb{K}}} = \frac{2(\sqrt{3}/2)^4}{\sqrt{256d^3}} = \frac{9}{128d\sqrt{d}}$. Quando $d = 2$, temos

$$\delta(\sigma_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}})) = \frac{9}{128 \cdot 2\sqrt{2}} \approx 0,02486.$$

Exemplo 4.3.1 Sejam $\mathbb{K} = \mathbb{Q}(\theta), \theta = \sqrt[4]{2}, \mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt[4]{2}]$ o anel dos inteiros algébricos de $\mathbb{K}$ e $X^4 - 2$ o polinômio irredutível de $\sqrt[4]{2}$ de θ sobre $\mathbb{Q}$. Consideremos o ideal $7\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^4 - 2$ fatora-se como:

$$X^4 - 2 \equiv (X + 2)(X + 5)(X^2 + 4)(\text{mod } 7\mathbb{Z}[X]).$$

Pelo Lema de Kummer temos que, $7\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, tal que $\mathfrak{p}_1 = (7, \theta + 2), \mathfrak{p}_2 = (7, \theta + 5)$ e $\mathfrak{p}_3 = (5, \theta^2 + 4)$, sendo esses os ideais primos acima de $7\mathbb{Z}$, cujo os graus residuais são 1 para $\mathfrak{p}_1, \mathfrak{p}_2$ e 2 para $\mathfrak{p}_3$ e as normas são 7, 7 e 7^2 , respectivamente. Além disso, $\mathfrak{D}_{\mathbb{K}} = \pm 256 \cdot 2^3$. Desta forma para calcularmos a densidade de centro do ideal primo $\sigma_{\mathbb{K}}(\mathfrak{p}_1)$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_{\mathbb{K}}$, temos que $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$ e como $\mathfrak{p}_1$ esta acima de $7\mathbb{Z}$ e $\theta \equiv -2(\text{mod } \mathfrak{p}_1)$, então $\alpha \in \mathfrak{p}_1$ se, e somente se, $a_0 - 2a_1 - 3a_2 - a_3 \in 7\mathbb{Z} = \mathfrak{p}_1 \cap \mathbb{Z}$. Daí nosso próximo passo é minimizar a forma quadrática.

$$|\sigma_{\mathbb{K}}(\alpha)|^2 = \frac{1}{2}\{2a_0^2 + 2a_1\theta^2 + 5a_2^2\theta^4 + 5a_3^2\theta^4 + (2a_0 + a_2\theta^2)^2 + (2a_1\theta + a_3\theta^3)^2\},$$

para valores de $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ que satisfazem a condição $a_0 - 2a_1 - 3a_2 - a_3 \in 7\mathbb{Z}$. Analisando todas as possibilidades, temos que a forma quadrática $|\sigma_{\mathbb{K}}(\alpha)|^2$ assume o menor valor quando $a_0 = 0, a_1 = 2, a_2 = 1, a_3 = 0$, e este valor é $10\theta^2 + 3\theta^4$, logo

$$\rho = \frac{\sqrt{10\theta^2 + 3\theta^4}}{2} \quad e \quad \delta(\sigma_K(\mathbf{p}_1))) = \frac{2 \left(\frac{\sqrt{10\theta^2 + 3\theta^4}}{2} \right)^4}{64 \cdot \sqrt{2} \cdot 7} \approx 0,0801. \quad \blacksquare$$

Sejam $d < 0$ um inteiro livre de quadrados, $\theta = \sqrt[4]{d}$, $K = \mathbb{Q}(\theta)$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . O polinômio irredutível de θ é $\text{irr}(\theta, \mathbb{Q}) = X^4 - d$ e suas raízes são $\theta, -i\theta, -\theta, i\theta$. Sejam, $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ as imersões de K em $\mathbb{C}$, tal que σ_1 é a inclusão, $\sigma_2(\theta) = -\theta, \sigma_3(\theta) = i\theta, \sigma_4(\theta) = -i\theta$. Dado $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$, como $t = 2$, temos que o homomorfismo canônico σ_K de K em $\mathbb{R}^4$ é dado por $\sigma_K(\alpha) = (\Re\sigma_1(\alpha), \Im\sigma_1(\alpha), \Re\sigma_2(\alpha), \Im\sigma_2(\alpha))$, e portanto,

$$|\sigma_K(\alpha)|^2 = \sigma_1(\alpha)\overline{\sigma_1(\alpha)} + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} = 2\{(a_0^2 - a_2^2\theta^4) + (-a_1i + a_3i\theta^4)\theta^2\}.$$

Esta forma quadrática é minimizada em $a_0 = 1, a_1 = a_2 = a_3 = 0$, assumindo o valor 3. Desta forma, $\rho = \frac{\sqrt{3}}{2}$. Dado que $\mathfrak{D}_K = \pm\mathcal{N}(f'(\theta)) = \pm 256d^3$, temos que a densidade de centro do reticulado $\sigma_K(\mathcal{O}_K)$ é $\delta(\sigma_K(\mathcal{O}_K)) = \frac{2^t \rho^n}{\mathfrak{D}_K} = \frac{2^2(\sqrt{3}/2)^4}{\sqrt{|256d^3|}} = \frac{1}{16|d|\sqrt{|d|}}$. Assim, quando $d = -1$, temos que

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{16} \approx 0,0625,$$

e quando $d = -2$, temos que

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{16 \cdot 2\sqrt{2}} \approx 0,0221.$$

Exemplo 4.3.2 Sejam $K = \mathbb{Q}(\theta), \theta = \sqrt[4]{-1}, \mathcal{O}_K = \mathbb{Z}[\sqrt[4]{-1}]$ o anel dos inteiros algébricos de K e $X^4 + 1$ o polinômio irredutível de θ sobre $\mathbb{Q}$. Consideremos o ideal $2\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^4 + 1$ fatora-se como:

$$X^4 + 1 \equiv (X + 1)^4 \pmod{2\mathbb{Z}[X]},$$

e pelo Lema de Kummer temos que, $2\mathcal{O}_K = \mathfrak{p}^4$, tal que, $\mathfrak{p} = (2, \theta + 1)$, sendo esse o único ideal primo acima de $2\mathbb{Z}$, cujo o grau residual é igual a 1 e a norma é 2. Além disso, $t = 2$ e $\mathfrak{D}_K = -256$. Desta forma, para calcularmos a densidade de centro do ideal primo $\sigma_K(\mathfrak{p})$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, temos que $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$, e como $\mathfrak{p}$ esta acima de $2\mathbb{Z}$ e $\theta \equiv -1 \pmod{\mathfrak{p}_1}$, então $\alpha \in \mathfrak{p}$ se, e somente se, $a_0 - a_1 + a_2 - a_3 \in 2\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Daí nosso próximo passo é minimizar a forma quadrática

$$|\sigma_K(\alpha)|^2 = 2\{(a_0^2 - a_2^2\theta^4) + (-a_1i + a_3^2i\theta^4)\theta^2\},$$

para valores de $a_0, a_1, a_2, a_3 \in \mathbb{Z}$ que satisfazem a condição $a_0 - a_1 + a_2 - a_3 \in 2\mathbb{Z}$. Analisando todas as possibilidades, temos que a forma quadrática $|\sigma_K(\alpha)|^2$ assume o menor valor quando $a_0 = 1, a_1 = -1, a_3 = a_2 = 0$, e este valor é igual a $1 - \theta^2$. Logo, $\rho = \frac{\sqrt{1 - \theta^2}}{2} e \delta(\sigma_K(\mathbf{p})) = \frac{2^2 \left(\frac{\sqrt{1 - \theta^2}}{2}\right)^4}{16.2} \approx 0,03125$. $\blacksquare$

4.4 Reticulados nas Quínticas

Nesta seção faremos o estudo de casos particulares de quínticas, com o objetivo de obter reticulados de posto 5 no $\mathbb{R}^5$. Deste modo nosso objetivo era a determinação do anel dos inteiros algébricos de $K = \mathbb{Q}(\sqrt[5]{d})$, com d livre de quadrados. Contudo, enfrentamos dificuldades na obtenção do mesmo, uma vez que envolve inúmeros cálculos. Porém determinamos o discriminante de K , a forma quadrática associada e a descrição dos reticulados obtidos em $\mathbb{R}^5$, via o homomorfismo canônico, a partir dos ideais ordinários de $\mathcal{O}_K$.

Seja d um inteiro livre de quadrados, $\theta = \sqrt[5]{d}$, $K = \mathbb{Q}(\theta)$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . Visto que $\mathcal{O}_K$ é um subconjunto de K então, dado $\alpha \in \mathcal{O}_K$ existem $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Q}$ tais que $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4$. O polinômio irredutível de θ é $\text{irr}(\theta, \mathbb{Q}) = X^5 - d$ e suas raízes são $\theta, \theta\xi, \theta\xi^2, \theta\xi^3, \theta\xi^4$ e o polinômio irredutível de ξ é $\text{irr}(\xi, \mathbb{Q}) = X^4 + X^3 + X^2 + X + 1$. Sejam $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5$ os monomorfismos de K em $\mathbb{C}$ tais que σ_1 é a inclusão, $\sigma_2(\theta) = \theta\xi, \sigma_3(\theta) = \theta\xi^2, \sigma_4(\theta) = \theta\xi^3$ e $\sigma_5(\theta) = \theta\xi^4$.

Dado $\alpha \in K$, se denotarmos $\alpha_i = \sigma_i(\alpha)$, para $i = 1, 2, 3, 4, 5$, temos que o polinômio característico de α é dado por

$$\begin{aligned} f_\alpha(X) &= (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)(X - \alpha_4)(X - \alpha_5) \\ &= X^5 - (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5)X^4 + (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_1\alpha_5 + \alpha_2\alpha_3 \\ &\quad + \alpha_2\alpha_4 + \alpha_2\alpha_5 + \alpha_3\alpha_4 + \alpha_3\alpha_5 + \alpha_4\alpha_5)X^3 - (\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_2\alpha_5 \\ &\quad + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_3\alpha_5 + \alpha_1\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_5 + \alpha_2\alpha_4\alpha_5 + \alpha_3\alpha_4\alpha_5)X^2 \\ &\quad + (\alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_5 + \alpha_1\alpha_2\alpha_4\alpha_5 + \alpha_1\alpha_3\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4\alpha_5)X \\ &\quad - (\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5). \end{aligned}$$

Fazendo os cálculos e as respectivas substituições, obtemos que

- $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 = 5a_0,$
- $\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_1\alpha_5 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_2\alpha_5 + \alpha_3\alpha_4 + \alpha_3\alpha_5 + \alpha_4\alpha_5 = 10a_0^2 - 5d(a_1a_4 + a_2a_3)$
- $\alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_2\alpha_5 + \alpha_1\alpha_3\alpha_4 + \alpha_1\alpha_3\alpha_5 + \alpha_1\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_5 + \alpha_2\alpha_4\alpha_5 + \alpha_3\alpha_4\alpha_5 = 10a_0^3 + 10d^2(a_3^2a_4 + a_2a_4^2) + 10d(a_1^2a_3 + a_1a_2^2) - 15d(a_0a_2a_3 + a_0a_1a_4),$
- $\alpha_1\alpha_2\alpha_3\alpha_4 + \alpha_1\alpha_2\alpha_3\alpha_5 + \alpha_1\alpha_2\alpha_4\alpha_5 + \alpha_1\alpha_3\alpha_4\alpha_5 + \alpha_2\alpha_3\alpha_4\alpha_5 = 5a_0^4 + 10d(a_0a_1^2a_3 + a_0a_1a_2^2) - 5d(3a_0^2a_1a_4 + a_1^3a_2 + 3a_0^2a_2a_3) + 10d^2(a_0a_3^2a_4 + a_0a_2a_4^2) - 5d^2(a_1a_3^3 + a_1a_2a_3a_4 + a_2^3a_4) + 5d^2a_2^2a_3^2 - 5d^3a_3a_4^3,$
- $\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5 = d(a_1^5 + 5a_0^2a_1a_2^2 + 5a_0^2a_1^2a_3 - 5a_0a_1^3a_2 - 5a_0^3a_2a_3 - 5a_0^3a_1a_4) + d^2(a_2^5 + 5a_1^2a_2a_3^2 + 5a_1^2a_2^2a_4 + 5a_0a_1^2a_4^2 + 5a_0a_2^2a_3^2 + 5a_0^2a_2a_4^2 + 5a_0^2a_3^2a_4 - 5a_0a_2^3a_4 - 5a_0a_1a_3^3 - 5a_0a_1a_2a_3a_4) + d^3(a_3^5 + 5a_1a_3^2a_4^2 + 5a_2^2a_3a_4^2 - 5a_1a_2a_4^3 - 5a_1a_3^2a_3 - 5a_2a_3^3a_4 - 5a_0a_3a_4^3) + d^4a_4^5.$

Portanto,

$$\begin{aligned} f_\alpha(X) = & X^5 - 5a_0X^4 + (10a_0^2 - 5d(a_1a_4 + a_2a_3))X^3 - (10a_0^3 + 10d^2a_3^2a_4 + 10d^2a_2a_4^2 \\ & + 10da_1^2a_3 + 10da_1a_2^2 - 15da_0a_2a_3 - 15da_0a_1a_4)X^2 + (5a_0^4 + 10da_0a_1^2a_3 \\ & + 10da_0a_1a_2^2 - 5d3a_0^2a_1a_4 - 5da_1^3a_2 - 15da_0^2a_2a_3 + 10d^2a_0a_3^2a_4 + 10d^2a_0a_2a_4^2 \\ & - 5d^2a_1a_3^3 - 5d^2a_1a_2a_3a_4 - 5d^2a_2^3a_4 + 5d^2a_2^2a_3^2 - 5d^3a_3a_4^3)X - (da_1^5 + 5da_0^2a_1a_2^2 \\ & + 5da_0^2a_1^2a_3 - 5da_0a_1^3a_2 - 5da_0^3a_2a_3 - 5da_0^3a_1a_4 + d^2a_2^5 + 5d^2a_1^2a_2a_3^2 + 5d^2a_1^2a_2^2a_4 \\ & + 5d^2a_0a_1^2a_4^2 + 5d^2a_0a_2^2a_3^2 + 5d^2a_0^2a_2a_4^2 + 5d^2a_0^2a_3^2a_4 - 5d^2a_0a_2^3a_4 - 5d^2a_0a_1a_3^3 \\ & - 5d^2a_0a_1a_2a_3a_4 + d^3a_3^5 + 5d^3a_1a_3^2a_4^2 + 5d^3a_2^2a_3a_4^2 - 5d^3a_1a_2a_4^3 - 5d^3a_1a_3^2a_3 \\ & - 5d^3a_2a_3^3a_4 - 5d^3a_0a_3a_4^3 + d^4a_4^5). \end{aligned}$$

Assim, segue da definição de elemento inteiro que $\alpha \in \mathcal{O}_K$ se, e somente se,



$$\left\{ \begin{array}{l} 5a_0 \in \mathbb{Z} \\ 10a_0^2 - 5da_1a_4 - 5da_2a_3 \in \mathbb{Z} \\ 10a_0^3 + 10d^2a_3^2a_4 + 10d^2a_2a_4^2 + 10da_1^2a_3 + 10da_1a_2^2 - 15da_0a_2a_3 - 15da_0a_1a_4 \in \mathbb{Z} \\ 5a_0^4 + 10da_0a_1^2a_3 + 10da_0a_1a_2^2 - 5d3a_0^2a_1a_4 - 5da_1^3a_2 - 15da_0^2a_2a_3 + 10d^2a_0a_3^2a_4 + \\ + 10d^2a_0a_2a_4^2 - 5d^2a_1a_3^3 - 5d^2a_1a_2a_3a_4 - 5d^2a_2^3a_4 + 5d^2a_2^2a_3^2 - 5d^3a_3a_4^3 \in \mathbb{Z} \\ da_1^5 + d5a_0^2a_1a_2^2 + 5da_0^2a_1^2a_3 - 5da_0a_1^3a_2 - 5da_0^3a_2a_3 - 5da_0^3a_1a_4 + d^2a_2^5 + 5d^2a_1^2a_2a_3^2 + \\ + 5d^2a_1^2a_2^2a_4 + 5d^2a_0a_1^2a_4^2 + 5d^2a_0a_2^2a_3^2 + 5d^2a_0^2a_2a_4^2 + 5d^2a_0^2a_3^2a_4 - 5d^2a_0a_2^3a_4 - 5d^2a_0a_1a_3^3 - \\ - 5d^2a_0a_1a_2a_3a_4 + d^3a_3^5 + 5d^3a_1a_3^2a_4^2 + 5d^3a_2^2a_3a_4^2 - 5d^3a_1a_2a_4^3 - 5d^3a_1a_2^3a_3 - 5d^3a_2a_3^3a_4 - \\ - 5d^3a_0a_3a_4^3 + d^4a_4^5 \in \mathbb{Z} \end{array} \right.$$

Proposição 4.4.1 Com as notações anteriores, temos que $\theta\mathcal{O}_K \cap \mathbb{Z} = d\mathbb{Z}$.

Demonstração: Se $d \in \mathbb{Z}$ e $d \in \theta\mathcal{O}_K$, então $d \in \theta\mathcal{O}_K \cap \mathbb{Z}$, e portanto $d\mathbb{Z} \subset \theta\mathcal{O}_K \cap \mathbb{Z}$. Por outro lado, seja $\theta\gamma \in \theta\mathcal{O}_K \cap \mathbb{Z}$. Assim existe $n \in \mathbb{Z}$, tal que $\theta\gamma = n$. Aplicando a norma, temos que $\mathcal{N}(\theta\gamma) = \theta^5\mathcal{N}(\gamma) = d\mathcal{N}(\gamma) = n^5$, o que implica que d divide n^5 , mas como d é livre de quadrados, segue que, d divide n . Logo $\theta\gamma \in d\mathbb{Z}$, e portanto, $\theta\mathcal{O}_K = d\mathbb{Z}$. $\blacksquare$

Além disso, temos

$$\begin{aligned} Tr_{K/Q}(\theta\gamma) &= \sigma_1(\theta\gamma) + \sigma_2(\theta\gamma) + \sigma_3(\theta\gamma) + \sigma_4(\theta\gamma) + \sigma_5(\theta\gamma) \\ &= \theta\sigma_1(\gamma) + \theta\xi\sigma_2(\gamma) + \theta\xi^2\sigma_3(\gamma) + \theta\xi^3\sigma_4(\gamma) + \theta\xi^4\sigma_5(\gamma) \\ &= \theta(\sigma_1(\gamma) + \xi\sigma_2(\gamma) + \xi^2\sigma_3(\gamma) + \xi^3\sigma_4(\gamma) + \xi^4\sigma_5(\gamma)) = \theta\omega, \end{aligned}$$

e visto que o traço de um elemento inteiro algébrico é sempre um número inteiro, temos que $\theta\omega = m$, com $m \in \mathbb{Z}$. Assim, $\omega = \frac{m}{\theta} \in K$. Por outro lado, temos que

$$\begin{aligned} Tr_{K/Q}(\alpha\theta) &= Tr_{K/Q}(a_0\theta + a_1\theta^2 + a_2\theta^3 + a_3\theta^4 + a_4\theta^5) = 5a_4d \in \mathbb{Z}, \\ Tr_{K/Q}(\alpha\theta^2) &= Tr_{K/Q}(a_0\theta^2 + a_1\theta^3 + a_2\theta^4 + a_3\theta^5 + a_4\theta^6) = 5a_3d \in \mathbb{Z}, \\ Tr_{K/Q}(\alpha\theta^3) &= Tr_{K/Q}(a_0\theta^3 + a_1\theta^4 + a_2\theta^5 + a_3\theta^6 + a_4\theta^7) = 5a_2d \in \mathbb{Z}, \\ Tr_{K/Q}(\alpha\theta^4) &= Tr_{K/Q}(a_0\theta^4 + a_1\theta^5 + a_2\theta^6 + a_3\theta^7 + a_4\theta^8) = 5a_1d \in \mathbb{Z}, \end{aligned}$$

e como $5a_0, 5a_1, 5a_2, 5a_3, 5a_4 \in \mathbb{Z}$, segue que $\alpha = \frac{b_0}{5} + \frac{b_1}{5}\theta + \frac{b_2}{5}\theta^2 + \frac{b_3}{5}\theta^3 + \frac{b_4}{5}\theta^4 \in \mathcal{O}_K$, com $b_i \in \mathbb{Z}$, $i = 0, 1, 2, 3, 4$. Daí pelo algoritmo da divisão, temos que

$$\alpha = c_0 + c_1\theta + c_2\theta^2 + c_3\theta^3 + c_4\theta^4 + \frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4,$$

com $c_i \in \mathbb{Z}$ e $r_i \in \{0, \pm 1, \pm 2\}$, para $i = 0, 1, 2, 3, 4$. Sendo assim, temos que α é inteiro algébrico se, e somente se, $\frac{r_0}{5} + \frac{r_1}{5}\theta + \frac{r_2}{5}\theta^2 + \frac{r_3}{5}\theta^3 + \frac{r_4}{5}\theta^4$ também for um inteiro algébrico. Assim, concluímos que $\alpha \in \mathcal{O}_K$ se, e somente se,

$$\left\{ \begin{array}{l} r_0 \in \mathbb{Z} \\ \frac{2}{5}r_0^2 - \frac{1}{5}dr_1r_4 - \frac{1}{5}dr_2r_3 \in \mathbb{Z} \\ \frac{2}{25}r_0^3 + \frac{2}{25}d^2r_3^2r_4 + \frac{2}{25}d^2r_2r_4^2 + \frac{2}{25}dr_1^2r_3 + \frac{2}{25}dr_1r_2^2 - \frac{3}{25}dr_0r_1r_4 - \frac{3}{25}dr_0r_2r_3 \in \mathbb{Z} \\ \frac{1}{125}r_0^4 + \frac{2}{125}dr_0r_1r_2^2 + \frac{2}{125}dr_0r_1^2r_3 + \frac{2}{125}d^2r_0r_2r_4^2 + \frac{2}{125}d^2r_0r_3^2r_4 + \frac{1}{125}d^2r_2^2r_3^2 - \\ - \frac{3}{125}dr_0^2r_1r_4 - \frac{3}{125}dr_0^2r_2r_3 - \frac{1}{125}d^2r_2^2r_4 - \frac{1}{125}d^2r_1r_2r_3r_4 \in \mathbb{Z} \\ \frac{1}{3125}dr_1^5 + \frac{1}{3125}d^2r_2^5 + \frac{1}{3125}d^3r_3^5 + \frac{1}{3125}d^4r_4^5 + \frac{1}{625}dr_1^2r_2r_3^2 + \frac{1}{625}dr_0^2r_1^2r_3 \\ + \frac{1}{625}d^2r_1^2r_2^2r_4 + \frac{1}{625}d^2r_0r_1^2r_4^2 + \frac{1}{625}d^2r_0r_2^2r_3^2 + \frac{1}{625}d^2r_0^2r_2r_4^2 + \frac{1}{625}d^2r_0^2r_3^2r_4 \\ + \frac{1}{625}d^3r_1r_3^2r_4^2 + \frac{1}{625}d^3r_2^2r_3r_4^2 - \frac{1}{625}dr_0r_1^3r_2 - \frac{1}{625}dr_0^3r_2r_3 - \frac{1}{625}dr_0^3r_1r_4 \\ - \frac{1}{625}d^2r_0r_2^3r_3 - \frac{1}{625}d^2r_0r_1r_3^3 - \frac{1}{625}d^2r_0r_1r_2r_3r_4 - \frac{1}{625}d^3r_1r_2r_4^3 - \frac{1}{625}d^3r_2r_3^3r_4 \\ - \frac{1}{625}d^3r_1r_2^3r_3 - \frac{1}{625}d^3r_0r_3r_4^3 \in \mathbb{Z} \end{array} \right.$$

Sejam d um inteiro livre de quadrados, $\theta = \sqrt[5]{d}$, $K = \mathbb{Q}(\theta)$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . Dado $\alpha \in K$, $\alpha = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3 + a_4\theta^4$, suponhamos que o número de homomorfismos imaginários seja $t = 1$, então o homomorfismo canônico σ_K de K em $\mathbb{R}^5$ é dada por

$$\sigma_K(\alpha) = (\alpha_1, \alpha_2, \alpha_3, \Re\sigma_4(\alpha), \Im\sigma_4(\alpha)),$$

e portanto, temos a seguinte forma quadrática

$$\begin{aligned}
|\sigma_K(\alpha)|^2 &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \sigma_4(\alpha)\overline{\sigma_4(\alpha)} = a_0a_1(2\theta + \theta\xi^3 + 2\theta\xi + 3\theta\xi^2) \\
&+ a_0a_1(2\theta^2 + \theta^2\xi + 2\theta^2\xi^2 + 3\theta^2\xi^4) + a_0a_3(2\theta^3 + \theta^3\xi^4 + 2\theta^3\xi^3 + 3\theta^3\xi) \\
&+ a_0a_4(2\theta^4 + \theta^4\xi^2 + 2\theta^4\xi^4 + 3\theta^4\xi^3) + a_1a_2(2\theta^3 + 3\theta^3\xi^3 + \theta^3\xi^2 + 2\theta^3\xi) \\
&+ a_1a_3(2\theta^4 + 3\theta^4\xi^4 + \theta^4\xi + 2\theta^4\xi^3) + a_1a_4(6\theta^5 + \theta^5\xi + \theta^5\xi^4) + a_2a_3(6\theta^5 \\
&+ \theta^5\xi^2 + \theta^5\xi^3) + a_2a_4(2\theta^6 + 3\theta^6\xi + \theta^6\xi^4 + 2\theta^6\xi^2) + a_3a_4(2\theta^7 + 3\theta^7\xi^2 \\
&+ \theta^7\xi^3 + 2\theta^7\xi^4) + a_1^2(\theta^2\xi^4 + \theta^2\xi^2 + 2\theta^2) + a_2^2(\theta^4\xi^4 + 2\theta^4 + \theta^4\xi^3) \\
&+ a_3^2(\theta^6\xi^2 + \theta^6\xi + 2\theta^6) + a_4^2(\theta^8\xi + 2\theta^8 + \theta^8\xi^3).
\end{aligned}$$

Esta forma quadrática é minimizada em $a_0 = 1, a_1 = a_2 = a_3 = a_4 = 0$, e assumindo o valor 4. Logo, $\rho = \frac{\sqrt{4}}{2} = 1$. Visto que $\mathfrak{D}_K = \pm\mathcal{N}(f'(\theta)) = 3125 \cdot d^4$, então a densidade

centro do reticulado $\sigma_K(\mathcal{O}_K)$ é dada por $\delta(\sigma_K(\mathcal{O}_K)) = \frac{2 \cdot \left(\frac{\sqrt{4}}{2}\right)^3}{\sqrt{3125 \cdot d^4}} = \frac{2}{25\sqrt{5} \cdot d^2}$. Assim,

quando $d = 2$, temos que $\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{50\sqrt{5}} \approx 0,0089$,

quando $d = 3$, temos que $\delta(\sigma_K(\mathcal{O}_K)) = \frac{2}{225\sqrt{5}} \approx 0,0039$.

Agora, se supormos que o número de homomorfismos imaginários seja $t = 2$, então o homomorfismo canônico de σ_K de $\mathbb{K}$ em $\mathbb{R}^5$ é dada por

$$\sigma_K(\alpha) = (\alpha_1, \Re\sigma_2(\alpha), \Im\sigma_2(\alpha), \Re\sigma_3(\alpha), \Im\sigma_3(\alpha)),$$

e portanto, temos a seguinte forma quadrática

$$\begin{aligned}
|\sigma_K(\alpha)|^2 &= \alpha_1^2 + \sigma_2(\alpha)\overline{\sigma_2(\alpha)} + \sigma_3(\alpha)\overline{\sigma_3(\alpha)} \\
&= 3a_0^2 + 3a_1^2 + 3a_2^2 + 3a_3^2 + 3a_4^2 + 2a_0a_1\theta + 2a_0a_2\theta^2 + 2a_0a_3\theta^3 + 2a_0a_4\theta^4 \\
&+ 2a_1a_2\theta^3 + 2a_1a_3\theta^4 + 2a_1a_4\theta + 2a_2a_3\theta + 2a_2a_4\theta^2 + 2a_3a_4\theta^2 + 3a_0^2 + 3a_1^2 \\
&+ 3a_2^2 + 3a_3^2 + 3a_4^2 + 2a_0a_1\theta + 2a_0a_2\theta^2 + 2a_0a_3\theta^3 + 2a_0a_4\theta^4 + 2a_1a_2\theta^3 \\
&+ 2a_1a_3\theta^4 + (2a_1\theta)(a_4\theta^4) + (2a_2\theta)(a_3\theta^4) + (2a_2\theta^3)(a_4\theta^3) + (2a_3\theta^3)(a_4\theta^4).
\end{aligned}$$

Esta forma quadrática é minimizada em $a_0 = 1, a_1 = a_2 = a_3 = a_4 = 0$, e assume o valor 3. Assim $\rho = \frac{\sqrt{3}}{2}$. Visto que $\mathfrak{D}_K = \pm\mathcal{N}(f'(\theta)) = 3125 \cdot d^4$, então a densidade de centro do reticulado $\sigma_K(\mathcal{O}_K)$ é dada por

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{2 \cdot \left(\frac{\sqrt{3}}{2}\right)^3}{\sqrt{3125 \cdot d^4}} = \frac{3\sqrt{3}}{100\sqrt{5} \cdot d^2} = \frac{9}{100\sqrt{15} \cdot d^2},$$

e quando $d = 2$, temos que $\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{50\sqrt{5}} \approx 0,0058$.

Bibliografia

- [1] Conway, J.H. and Sloane, N.J.A. *Sphere Packings, Lattices and Groups*. Springer, New York, 1999.
- [2] Endler, O. *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro 1986.
- [3] Flores, A.L. *Reticulados em Corpos Abelianos*. Dissertação de Doutorado, FEEC/UNICAMP, 2000.
- [4] Herstein, I.N., *Tópicos de Álgebra*. Editora Polígono S.A.1970.
- [5] Samuel, P. *Algebraic Theory of Numbers*. Hermana, Paris, 1967.
- [6] Silva, C. V. *Reticulados de Posto 4 em Corpos de Números*. Dissertação de Mestrado, IBILCE - UNESP, São José do Rio Preto, 2001.
- [7] Stewart, I., Tall, D. *Algebraic Number Theory*. Chapman & Hall, New York,1987.
- [8] Vicente, J. P. G. *Reticulados de Posto 3 em Corpos de Números*. Dissertação de Mestrado, IBILCE - UNESP, São José do Rio Preto, 2000.



