

Joselma Pinheiro Gonçalves Vicente

Reticulados de Posto 3 em Corpos de Números



1910000923



Universidade Estadual Paulista
Campus de São José do Rio Preto
Instituto de Biociências, Letras e Ciências
Exatas

Reticulados de Posto 3 em Corpos de Números

por

Joselma Pinheiro Gonçalves Vicente

sob orientação do

Prof. Dr. Trajano Pires da Nóbrega Neto



Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como requisito parcial para obtenção do título de Mestre em ciências Matemáticas - Área de concentração Matemática.

Maio/2000
São José do Rio Preto - SP

Reticulados de Posto 3 em Corpos de Números

por

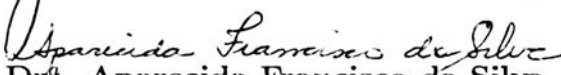
Joselma Pinheiro Gonçalves Vicente

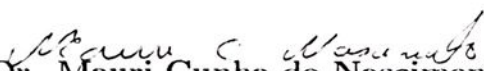
Dissertação apresentada ao Departamento de Matemática - IBILCE - UNESP, como requisito parcial para obtenção do título de Mestre em Ciências Matemáticas - Área de Concentração Matemática.

Área de Concentração: Álgebra

Aprovada por:


Prof. Dr. Trajano Pires da Nóbrega Neto


Prof^a. Dr^a. Aparecida Francisco da Silva


Prof. Dr. Mauri Cunha do Nascimento

Universidade Estadual Paulista
Campus de São José do Rio Preto
Instituto de Biociências, Letras e Ciências Exatas

Maio/2000



Agradecimentos

- Ao meu orientador prof. Dr.Trajano Pires da Nóbrega Neto, pela paciência, dedicação e amizade.
- Aos docentes do Departamento de Matemática da UNESP de São José do Rio Preto, pelo conhecimento transmitido.
- Aos docentes do Departamento de Matemática da UFMT, Campus de Rondonópolis, pela compreensão que me foi dispensada.
- À todos os amigos que de alguma forma contribuíram para a conclusão deste trabalho.
- À CAPES e à FAPESP, pelo apoio financeiro.



Dedico

Aos meus pais
Adildo e Jacy,
ao Tati e
aos meus filhos
Thaís e Thales.

Sumário

0.1	Histórico	iii
0.2	Motivação	iv
0.3	Descrição do Trabalho	v
1	Corpos de Números	1
1.1	Elementos Inteiros sobre um Anel	2
1.2	Elementos Algébricos sobre um Corpo	7
1.3	Base Integral	19
1.4	Norma e Traço	22
1.5	Fatoração de Ideais	24
1.6	Norma de um Ideal	32
2	Reticulados em Corpos de Números	37
2.1	Corpos Quadráticos	38
2.2	Corpos Ciclotômicos	41
2.2.1	Polinômios Ciclotômicos	41
2.2.2	Base Integral e Discriminante	46
2.3	Corpos Abelianos	56
2.4	Reticulados	58
2.5	O Homomorfismo Canônico	61

3 Cúbicas e Aplicações **68**

3.1 Reticulados em Corpos Quadráticos 70

3.2 Reticulados em Corpos Ciclotômicos 73

3.3 Cúbicas não Galoisianas 76

3.4 Cúbicas Galoisianas 83

3.5 Outros Reticulados de Posto 3 86

Referencias Bibliográficas **91**

Índice de Símbolos

$\mathbb{N}$: o conjunto dos números naturais

$\mathbb{Z}$: o conjunto dos números inteiros

$\mathbb{Q}$: o conjunto dos números racionais

$\mathbb{R}$: o conjunto dos números reais

$\mathbb{C}$: o conjunto dos números complexos

$\ker f$: núcleo do homomorfismo f

$\operatorname{im} f$: imagem do homomorfismo f

∂f : grau do polinômio f

$[L : K]$: grau de L sobre K

$(E : F)$: índice de F em E

$\prod$: produto

$\sum$: soma

$\det A$: determinante da matriz A

(a_{ij}) : matriz

$f_\alpha(X)$: polinômio característico de α

$\Delta[\alpha_1, \dots, \alpha_n]$: discriminante de uma n -upla

$\mathcal{O}_K$: anel dos inteiros algébricos do corpo de números K

$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{p}, \dots$: ideais

$\mathfrak{a}^{-1}$: inverso de um ideal fracionário

$N(\mathfrak{a})$: norma de $\mathfrak{a}$

$\#X$: cardinalidade do conjunto X

$A \times B$: produto cartesiano de A por B

(r, s) : maior divisor comum de r e s

$\phi(n)$: número de elementos de $(\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ ou ϕ de Euler

$A[X]$: anel dos polinômios sobre A em X

$K(\alpha_1, \dots, \alpha_n)$: corpo obtido pela adjunção $\alpha_1, \dots, \alpha_n$ a K



$R[\alpha_1, \dots, \alpha_n]$: anel gerado por R e $\alpha_1, \dots, \alpha_n$

$\frac{R}{I}$: anel quociente

$\forall$: para todo

$\exists$: existe

$\xi_n : e^{2\pi i/n} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$

$\bar{x}$: conjugado complexo do elemento x

$\mathcal{D}_K$: discriminante absoluto do corpo K

$T_{L/K}$: traço com relação a L e K

$N_{L/K}$: norma com relação a L e K

$|a| = \sqrt{a\bar{a}} = \sqrt{a_1^2 + \dots + a_n^2}$, $a = (a_1, \dots, a_n) \in \mathbb{R}^n$

$\langle x_1, \dots, x_n \rangle$: ideal gerado por $x_1, \dots, x_n$

$\underline{X} = (X_1, \dots, X_n) \in \mathbb{R}^n$



Introdução

0.1 Histórico

Entende-se por Empacotamento Esférico a disposição de esferas de mesmo raio no espaço euclidiano $\mathbb{R}^n$ de tal modo que a interseção de duas delas tenha no máximo um ponto.

A forma de dispor essas esferas de modo a cobrir a maior parte do espaço, sempre foi um desafio para os matemáticos e mereceu citação de Hilbert em 1900 citando-o como o 18º Problema de uma seleta lista de desafios que viriam ocupar destaque no desenvolvimento da ciência moderna.

Muitas teorias evoluíram tendo o 18º Problema de Hilbert como inspiração. Vários modelos matemáticos foram descritos com a finalidade de se obter empacotamentos esféricos com alta densidade; muitas cotas foram estabelecidas.

Dentre os empacotamentos esféricos aqueles cujo conjunto dos centros das esferas constituía um subgrupo discreto de $\mathbb{R}^n$ despertaram particular interesse e passaram a se chamar empacotamentos reticulados. A teoria de $\mathbb{Z}$ -módulos passou a ser intensamente utilizada na busca de melhores resultados.

Entretanto na maioria das dimensões os empacotamentos mais densos conhecidos são 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 aquele descrito por Minkowski, no final do século XIX / início do século XX. Nesta época Minkowski estava interessado em provar a finitude do Grupo das Classes, quando desenvolvia a sua teoria de Corpos de Classes.

Tal modelo consistia em; dados um corpo de números K de grau n , o seu anel de inteiros algébricos A , obtem-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 A 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, oriunda da função traço. Como pode ser visto, o problema do empacotamento reticulado, via modelo de Minkowski, encontrou na Teoria Algébrica dos Números ferramentas que viabilizaram o efetivo cálculo da densidade de centro.

0.2 Motivação

A dedicação na busca de empacotamento reticulado via método de Minkowski mostrou seus primeiros resultados com os trabalhos de Maurice Craig. Outras colaborações foram surgindo a medida que o modelo se mostrava mais promissor.

Os principais resultados publicados em revistas especializadas mostram o anel dos inteiros algébricos de corpos ciclotômicos como o universo capaz de produzir ideais ordinários não nulos cuja representação geométrica coincidam com os reticulados mais densos conhecidos e até assumam novos recordes.



Isso limita o estudo às dimensões da forma $\phi(n)$, ϕ a função de Euler. Tal restrição se justifica pela complexidade do problema quando este é tratado em outros corpos, mesmos nos corpos abelianos.

Para situações como esta, começam a surgir resultados promissores em corpos abelianos, cujo objetivo é fornecer contribuições do modelo de Minkowski em todas as dimensões cujas respectivas densidades de empacotamento estejam dentre as maiores conhecidas.

Este trabalho tem como propósito focar a dimensão 3, descrevendo a teoria necessária para sua plena compreensão e efetuando cálculos de casos particulares cujo objetivo é encorajar o leitor a buscar a sua própria contribuição para esta e outras dimensões.

0.3 Descrição do Trabalho

Em todo este trabalho os anéis considerados são comutativos e com elemento unidade. Além disso cada resultado aqui enunciado será acompanhado de um número que representa uma referência que o contém. Quando tal número não aparece é porque se trata de resultado de domínio público.

O Capítulo 1, visa atender aos leitores com menos conhecimentos em Teoria Algébrica dos Números, ao nível das referências [6, 7].

Aqui introduzimos os conceitos de corpos de números, inteiros algébricos, discriminante, base integral, norma e traço de um elemento, fatoração de um ideal primo, norma de ideal e outros conceitos indispensáveis ao desenvolvimento do Capítulo.

Com relação ao conjunto dos elementos de um corpo de números K de grau n que são inteiros sobre $\mathbb{Z}$, provamos que este é um Domínio de Dedekind



(Teorema 1.9) e é um $\mathbb{Z}$ -módulo livre de posto n (Teorema 1.7).

A base integral tem a sua importância no cálculo do discriminante, que é sempre um número inteiro não nulo e seu valor independe da base integral escolhida.

Quanto a fatoração de ideais, mostramos que o conjunto dos ideais fracionários do anel dos inteiros algébricos de um corpo de números K , é um grupo abeliano multiplicativo (Teorema 1.10) e ainda, que todo ideal ordinário deste mesmo anel é fatorado, de modo único, como um produto de ideais primos (Teorema 1.11).

Concluindo o Capítulo, definimos norma de um ideal do anel dos inteiros algébricos de um corpo de números e mostramos que a função norma é multiplicativa.

No Capítulo 2, caracterizamos os anéis dos inteiros algébricos e o discriminante dos corpos quadráticos, ou seja, corpos de números de grau 2, corpos ciclotômicos e apresentamos demonstrações do Teorema 2.2 e do Teorema 2.3 usando apenas argumentos aritméticos.

Introduzimos em seguida as definições de reticulado, empacotamento esférico, densidade de empacotamento, densidade de centro e apresentamos o Método de Minkowski (O Homomorfismo Canônico), para obtenção de reticulados via representação geométrica de ideais ordinários do anel dos inteiros algébricos de um corpo de números. O Teorema 2.7 constitui um importante resultado deste Capítulo, pois mostra que a representação geométrica de um ideal é um reticulado e explicita a fórmula geral para o cálculo da densidade de centro destes reticulados.

O Capítulo 3 é dedicado às cúbicas e suas aplicações; nele empregamos toda a teoria desenvolvida nos Capítulos anteriores e tem como principal objetivo calcular a densidade de centro de reticulados de posto 3 em $\mathbb{R}^3$.



Iniciamos com reticulados em corpos quadráticos, em seguida estudamos reticulados em corpos ciclotômicos e finalmente nos casos particulares de cúbicas. Nas cúbicas enfocamos as cúbicas não galoisianas da forma $\mathbb{Q}(\sqrt[3]{d})$, d inteiro livre de quadrados e as cúbicas galoisianas contidas em $\mathbb{Q}(\xi_{p^r})$, p primo, $r \geq 1$. Em ambos os casos calculamos a densidade de centro de alguns reticulados de posto 3.

Finalizando, estudamos os módulos de posto 3 e empregamos um método que é uma generalização do Método de Minkowski, para obter reticulados via representação geométrica de $\mathbb{Z}$ -módulos de anéis de inteiros algébricos.



Capítulo 1

Corpos de Números

Neste Capítulo, introduzimos os resultados básicos da Teoria Algébrica dos Números, tendo em vista fornecer pré-requisitos para uma melhor compreensão dos capítulos subsequentes e também a familiarização com a notação aqui adotada. Admitimos que o leitor tenha conhecimentos elementares de Estruturas Algébricas e Álgebra Linear.

Iniciamos com as definições de elementos inteiros sobre um anel, algébricos sobre um corpo e observamos as relações entre estes elementos de forma geral. Em seguida definimos corpo de números e alguns de seus principais parâmetros tais como discriminante, base integral, norma e traço. A última seção deste Capítulo é dedicada ao estudo da fatoração de ideais, onde definimos norma de ideais.

Com o propósito de tornar este trabalho o mais auto suficiente possível incluiremos todas as demonstrações cujo nível de dificuldade seja compatível com esta dissertação.

O fato de que o conjunto dos inteiros algébricos de um corpo de números constituir um anel e ser um $\mathbb{Z}$ -módulo livre de posto n e que todo ideal deste anel pode ser fatorado de modo único como um produto de ideais primos,



representam os principais resultados deste Capítulo.

As principais referências aqui utilizadas são [6, 7], tanto em nível de conteúdo como de notação.

1.1 Elementos Inteiros sobre um Anel

Sejam R um anel e A um subanel de R . Dizemos que um elemento x de R é *inteiro* sobre A se este é raiz de um polinômio mônico com coeficientes em A .

Exemplo 1.1 O elemento $x = \sqrt{2} + \sqrt{3}$ é inteiro sobre $\mathbb{Z}$, pois é raiz do polinômio

$$X^4 - 10X^2 + 1 \in \mathbb{Z}[X].$$

Teorema 1.1 [7] *Sejam R um anel, A um subanel de R e $x \in R$. Então as seguintes condições são equivalentes:*

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

Demonstração. (1) $\Rightarrow$ (2) Temos que x é inteiro sobre A , então x satisfaz uma equação

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0;$$

com $a_i \in A$; $i = 1, \dots, n-1$. Esta equação é chamada *Equação de Dependência Inteira de x* . Assim

$$x^n = -(a_{n-1}x^{n-1} + \cdots + a_1x + a_0),$$



ou seja, x^n é uma combinação linear dos elementos $1, x, \dots, x^{n-1}$. Logo

$$x^n \in \langle 1, x, \dots, x^{n-1} \rangle.$$

Mostremos que $x^j \in \langle 1, x, \dots, x^{n-1} \rangle$ para $j \geq n$, por indução sobre j . Para $j = n$, o resultado já é satisfatório e se vale para j , mostremos que vale para $j + 1$. Sendo

$$x^j = b_0 + b_1x + \dots + b_{n-1}x^{n-1};$$

com $b_i \in A$, então

$$\begin{aligned} x^{j+1} &= b_0x + b_1x^2 + \dots + b_{n-2}x^{n-1} + b_{n-1}x^n \\ &= -b_{n-1}a_0 + (b_0 - b_{n-1}a_1)x + \dots + (b_{n-2} - b_{n-1}a_{n-1})x^{n-1} \end{aligned}$$

e assim $x^{j+1} \in \langle 1, x, \dots, x^{n-1} \rangle$ e $A[x] \subset \langle 1, x, \dots, x^{n-1} \rangle$. Por outro lado, $\langle 1, x, \dots, x^{n-1} \rangle \subset A[x]$ e portanto o resultado está provado.

(2) $\Rightarrow$ (3) Basta tomar $B = A[x]$.

(3) $\Rightarrow$ (1) Sejam $B = \langle y_1, \dots, y_n \rangle$, $x \in B$ e $y_i \in B$. Então $xy_i \in B$, pois B é subanel de R e

$$xy_i = \sum_{j=1}^n a_{ij}y_j, i = 1, \dots, n; a_{ij} \in A, 1 \leq i, j \leq n.$$

Logo $xy_i - \sum_{j=1}^n a_{ij}y_j = 0$, $i = 1, \dots, n$ é um sistema linear homogêneo nas variáveis $y_1, \dots, y_n$, ou seja, $\sum_{j=1}^n (\delta_{ij}x - a_{ij})y_j = 0$, sendo $\delta = 1$ se $i = j$ e 0 se $i \neq j$.

Sejam

$$C = (\delta_{ij}x - a_{ij})_{n \times n}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \text{ e } d = \det C.$$

Sendo $(adj C).C = d.I$; onde $adj C$ é a matriz adjunta de C e I a matriz identidade, segue que, $d.Y = 0$, logo $dy_i = 0$ para todo i . Consequentemente, para todo $b \in B$, $b = \sum_{i=1}^n b_i y_i$; $b_i \in A$, então

$$db = d \sum_{i=1}^n b_i y_i = \sum_{i=1}^n b_i (dy_i) = 0,$$

em particular para $1 \in B$, de onde $d = 0$.

Seja $f(X) \in A[X]$ tal que $f(x) = \det C$, então é possível ver que $f(X)$ é mônico. Portanto x é inteiro sobre A . $\square$

Proposição 1.1 [7] *Sejam R um anel, A um subanel de R e $x_1, \dots, x_n$ elementos de R tais que x_i é inteiro sobre $A[x_1, \dots, x_{i-1}]$, $i = 2, \dots, n$. Então $A[x_1, \dots, x_n]$ é um A -módulo finitamente gerado.*

Demonstração. A demonstração é feita por indução sobre n . Para $n = 1$ é imediata, pelo Teorema 1.1. Suponhamos $n > 1$ e que a afirmação seja verdadeira para $n - 1$ elementos.

Seja $A[x_1, \dots, x_n] = B[x_n]$, sendo $B = A[x_1, \dots, x_{n-1}]$. Por hipótese de indução B é um A -módulo finitamente gerado, isto é, $B = \sum_{i=1}^s A y_i$. Visto que x_n é inteiro sobre B então $B[x_n]$ é um B -módulo finitamente gerado, isto é, $B[x_n] = \sum_{j=1}^t B z_j$. Então

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

Assim,

$$A[x_1, \dots, x_n] = \langle y_i z_j, 1 \leq i \leq s, 1 \leq j \leq t \rangle.$$

De fato, seja $\alpha \in B[x_n]$, $\alpha = \sum_{i=1}^t b_i z_i$, com $b_i \in B$. Por outro lado, podemos escrever,

$$b_i = \sum_{j=1}^s a_{ij} y_j, i = 1, \dots, t, a_{ij} \in A,$$

e daí,

$$\alpha = \left(\sum_{j=1}^s a_{ij} y_j \right) z_i = \left(\sum_{j=1}^s a_{1j} y_j \right) z_1 + \cdots + \left(\sum_{j=1}^s a_{tj} y_j \right) z_t.$$

Portanto $A[x_1, \dots, x_n]$ é um A -módulo finitamente gerado. $\square$

Esta sequência de resultados será utilizada para a demonstração da Proposição seguinte, que caracteriza o conjunto dos elementos de R inteiros sobre um subanel A de R .

Proposição 1.2 [7] *Sejam R um anel e A um subanel de R . Então o conjunto A' dos elementos de R inteiros sobre A é um subanel de R contendo A .*

Demonstração. De fato, sejam x e y elementos de R inteiros sobre A . Então $A[x, y]$ é um A -módulo finitamente gerado contendo A , $x + y$, $x - y$ e xy . Além disso, A está contido em A' , pois dado $c \in A$, c é raiz do polinômio mônico $X - c \in A[X]$. $\square$

Denominamos por *fecho inteiro* de A em R , o anel A' acima definido e quando R for um domínio, chamamos de fecho inteiro de R , ao fecho inteiro de R em seu corpo de frações.

Sejam R um anel e A um subanel de R . Dizemos que R é inteiro sobre A , se todo elemento de R é inteiro sobre A . Dentre os anéis que satisfazem esta condição, citamos o anel dos Inteiros de Gauss contendo $\mathbb{Z}$, pois todo elemento $a + bi$ de $\mathbb{Z}[i]$ é raiz do polinômio

$$X^2 - 2aX + (a^2 + b^2) \in \mathbb{Z}[X].$$

Proposição 1.3 [7] *Sejam R um anel, B um subanel de R e A um subanel de B . Se R é inteiro sobre B e B é inteiro sobre A , então R é inteiro sobre A .*



Demonstração. Seja $x \in R$. Visto que R é inteiro sobre B existem $b_0, \dots, b_{n-1} \in B$ tais que

$$b_0 + b_1x + \dots + b_{n-1}x^{n-1} + x^n = 0 \quad (*)$$

Fazendo $C = A[b_0, \dots, b_{n-1}]$, segue por $(*)$ que x é inteiro sobre C , logo $C[x]$ é um C -módulo finitamente gerado. Por hipótese $b_0, \dots, b_{n-1}$ são inteiros sobre A , daí $x = b_0, \dots, x_{n-1} = b_{n-1}$ e $x_n = x$ é uma sequência satisfazendo as condições da Proposição 1.1 e assim $C[x]$ é um A -módulo finitamente gerado. Logo $A[x] \subset C[x] \subset R$ e pelo Teorema 1.1, x é inteiro sobre A . Portanto R é inteiro sobre A . $\square$

Dizemos que um anel R é *integralmente fechado* quando R é um domínio e é seu próprio fecho inteiro.

Em outras palavras, um anel R é integralmente fechado se todo elemento do seu corpo de frações que é inteiro sobre R está em R .

Observação 1.1 *Todo anel fatorial 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 $(a, b) = 1$. Sendo x inteiro, x satisfaz a equação de dependência inteira

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0;$$

com $a_i \in A$, $i = 1, \dots, n-1$. Multiplicando esta equação por b^n , obtemos

$$a^n + a_{n-1}a^{n-1}b + \dots + a_1ab^{n-1} + a_0b^n = 0.$$

Assim,

$$a^n = b(-a_{n-1}a^{n-1} - \dots - a_1ab^{n-2} - a_0b^{n-1}),$$

logo b divide a^n . Visto que $(a, b) = 1$, e aplicando o Lema de Euclides sucessivas vezes, concluímos que b divide a , isto é, b é um elemento inversível do anel A , e assim $x = \frac{a}{b} \in A$. Portanto A é integralmente fechado.

1.2 Elementos Algébricos sobre um Corpo

Sejam R um anel e K um subcorpo de R . Dizemos que um elemento x de R é *algébrico* sobre K , se este é raiz de um polinômio não nulo, com coeficientes em K . Se todo elemento de R for algébrico sobre K , dizemos que R é algébrico sobre K . Um elemento de R não algébrico sobre K é dito *transcendente* sobre K .

Exemplo 1.2 O elemento $x = \sqrt{3} + \sqrt{-5}$ é algébrico sobre $\mathbb{Q}$, pois é raiz do polinômio

$$X^4 + 4X^2 + 64 \in \mathbb{Q}[X].$$

Segundo a definição, sendo x algébrico sobre um corpo K , x satisfaz uma equação do tipo:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0;$$

com $a_i \in K$, $a_n \neq 0$. Multiplicando a equação acima por a_n^{-1} , obtemos uma equação de dependência inteira,

$$x^n + a_n^{-1} a_{n-1} x^{n-1} + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0 = 0$$

e, portanto, sobre um corpo, o conceito de elemento algébrico coincide com o de inteiro.

Uma extensão L de K é dita *algébrica* se todo elemento de L é algébrico sobre K .

Definição 1.1 Dados $K \subset L$ corpos e α um elemento de L , o conjunto de todas as expressões polinomiais em α e coeficientes em K será denotado por $K[\alpha]$.



Dados um corpo L e um subcorpo K de L , a *dimensão* de L como espaço vetorial sobre K é chamada *grau* de L sobre K e denotada por $[L : K]$. Se $[L : K]$ é finito, então L é uma *extensão algébrica* de K e desde que sobre um corpo; algébrico significa inteiro, então podemos usar os resultados obtidos anteriormente de elementos inteiros para elementos algébricos. Assim, para $K \subset R$ e $x \in R$, x é algébrico sobre K se, e somente se, $[K[x] : K]$ é finito.

Um resultado muito útil de extensões algébricas é que 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 vale $[F : K] = [F : L].[L : K]$. Para ver isto, basta considerar o conjunto

$$S = \{v_i u_j; \{v_1, \dots, v_r\} \text{ é base de } F/L \text{ e } \{u_1, \dots, u_s\} \text{ é base de } L/K\}$$

e verificar que, além de ser uma base da extensão F de K , sua cardinalidade é $[F : L].[L : K]$.

Sejam R um anel, K um subcorpo de R e x um elemento de R . Consideremos o homomorfismo de anéis $\sigma_x : K[X] \rightarrow R$ definido por $\sigma_x(a) = a; \forall a \in K$ e $\sigma_x(X) = x$. Assim,

$$\ker \sigma_x = \{f(X) \in K[X]; f(x) = 0\} \text{ e}$$

$$\text{Im } \sigma_x = \{\sigma(f(X)); f(X) \in K[X]\} = \{f(x); f(X) \in K[X]\} = K[x].$$

Através deste homomorfismo podemos redefinir elemento algébrico sobre K da seguinte forma: x é algébrico sobre K se $\ker \sigma_x \neq \{0\}$. Quando x é transcendente sobre K , $K[x] \simeq K[X]$.

Sabemos que $K[X]$ é um anel principal, em particular $\ker \sigma_x$ é um ideal principal, gerado por um polinômio $f(X) \in K[X]$, ou seja, $\ker \sigma_x = \langle f(X) \rangle$.



Sendo x transcendente então $f(X)$ é o polinômio nulo e se x é algébrico $f(X)$ 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 $\ker \sigma_x$, $f(X)$ tem grau mínimo dentre os polinômios que se anulam em x , sendo chamado de polinômio minimal de x sobre K . Assim descrito $f(X)$ é irredutível sobre K e denotamos por $\text{irr}(x, K)$ e $\partial \text{irr}(x, K) = [K(x) : K]$.

Definição 1.2 *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:*

1. $K \subset L$,
2. $f(X)$ se fatora sobre L como produto de polinômios de grau 1 e
3. L é o menor corpo satisfazendo os itens acima.

Exemplo 1.3 *O corpo $L = \mathbb{Q}(\sqrt[3]{2}, \xi_3)$ é o corpo de raízes do polinômio $X^3 - 2 \in \mathbb{Q}[X]$ e $\xi_3 = e^{2\pi i/3}$.*

Uma extensão L de K é dita simples se existe $\theta \in L$ tal que $L = K(\theta)$.

Teorema 1.2 [4] *Sejam K um corpo e $f(X) \in K[X]$ um polinômio não constante. Então existe uma extensão simples L de K contendo uma raiz de $f(X)$.*

Demonstração. Suponhamos, sem perda de generalidade, que $f(X)$ é irredutível. Logo $\langle f(X) \rangle$ é um ideal maximal de $K[X]$ e, portanto, $\frac{K[X]}{\langle f(X) \rangle}$ é um corpo, que denotamos por M .

Seja $\sigma : K[X] \rightarrow M$ a projeção canônica, ou seja,

$$\sigma(g(X)) = g(X) + \langle f(X) \rangle = \overline{g(X)},$$

para qualquer $g(X) \in K[X]$. Considere a restrição de σ a K , isto é, $\sigma|_K(a) = \sigma(a)$, para qualquer $a \in K$ e mostremos que $\sigma|_K$ é injetiva. De fato, se $\sigma|_K(a) = \bar{a} = \bar{0}$ então $a \in \langle f(X) \rangle$. Visto que $\partial f(X) > 0$, a única constante no ideal gerado por $\langle f(X) \rangle$ é a constante nula, ou seja, $a = 0$. Assim, $K \simeq \text{Im } \sigma|_K$ e este isomorfismo permite associar $a \in K$ com $\bar{a}$ em M , conseqüentemente identificamos K com sua imagem em M . Por outro lado, desde que para qualquer $h(X) \in K[X]$, $\sigma(h(X)) = h(\sigma(X))$ então resta mostrar que $x = X + \langle f(X) \rangle$ é uma raiz de $f(X)$. Sendo $x = \sigma(X)$, temos que

$$f(x) = f(\sigma(X)) = \sigma(f(X)) = \overline{f(X)} = \bar{0}$$

logo x é uma raiz de $f(X)$ e $x \in M$. Agora vamos mostrar que $\frac{K[X]}{\langle f(X) \rangle} \simeq K(x)$. Considere

$$\begin{aligned} \varphi: K[X] &\rightarrow K(x) \\ l(X) &\rightarrow l(x). \end{aligned}$$

É óbvio que φ é sobrejetor. Mostremos que $\ker \varphi = \langle f(X) \rangle$. Seja $h(X) \in \ker \varphi$, então $\varphi(h(X)) = h(x) = 0$ e assim $h(X)$ é múltiplo de $f(X)$, isto é, $h(X) \in \langle f(X) \rangle$. Reciprocamente, se $h(X) \in \langle f(X) \rangle$ então existe $g(X) \in K[X]$ tal que $h(X) = f(X)g(X)$, logo $h(X) \in \ker \varphi$. Portanto $M \simeq K(x)$ e visto que são espaços vetoriais de mesma dimensão finita sobre K , concluímos que $K(x) = M$. Considerando $L = M$ segue-se o resultado. $\square$

Em consequência deste Teorema temos o seguinte

Corolário 1.1 [4] *Para todo polinômio não constante $g(X) \in K[X]$, existe um corpo de raízes L de $g(X)$ sobre K .*

Demonstração. A demonstração é feita por indução sobre o grau de $g(X)$. Se $\partial g(X) = 1$ então o resultado segue facilmente. Suponhamos agora



que seja verdadeiro para todo polinômio com grau menor do que n e que $\partial g(X) = n$. Seja M uma extensão de K que contém uma raiz x de $g(X)$. Em M , $g(X) = (X - x)h(X)$, $\partial h(X) = n - 1$. Aplicando a hipótese de indução, existe o corpo de raízes L de $h(X)$ sobre M , com $M = K(x)$ e

$$L = M(x_2, \dots, x_n) = K(x, x_2, \dots, x_n),$$

com $x, x_2, \dots, x_n$ as raízes de $g(X)$. □

Proposição 1.4 [4] *Sejam K um corpo, $f(X) \in K[X]$ um polinômio irredutível e α, β duas raízes de $f(X)$ em alguma extensão de K . Então existe um único K -isomorfismo $\varphi : K(\alpha) \rightarrow K(\beta)$ tal que $\varphi(\alpha) = \beta$.*

Demonstração. Dado $x \in K(\alpha)$, seja $g(X) \in K[X]$ tal que $x = g(\alpha)$. Consideremos a aplicação $\varphi : K(\alpha) \rightarrow K(\beta)$ tal que $\varphi(a) = a$; $\forall a \in K$, $\varphi(\alpha^i) = \beta^i$, $i = 1, \dots, n - 1$ e estendemos φ por linearidade à todo $K(\alpha)$, isto é, $\varphi(g(\alpha)) = g(\beta)$, para qualquer $g(X) \in K[X]$. Mostremos que φ está bem definida. Sejam $g(X), h(X) \in K[X]$ tal que $g(\alpha) = h(\alpha)$ então $g(\alpha) - h(\alpha) = 0$ daí, $(g - h)(\alpha) = 0$, logo $f(X)$ divide $(g - h)(X)$. Portanto $(g - h)(\beta) = 0$, ou seja, $g(\beta) = h(\beta)$.

O homomorfismo φ é um K -monomorfismo, pois se $\varphi(g(\alpha)) = g(\beta) = 0$, então $f(X)$ divide $g(X)$ e portanto $g(\alpha) = 0$ e a unicidade de φ decorre da sua construção. Agora mostremos que σ é único. De fato, seja

$$\begin{aligned} \sigma : K(\alpha) &\rightarrow K(\beta) \\ \alpha &\rightarrow \beta. \end{aligned}$$

Assim $\sigma(\alpha^j) = (\beta)^j$ e ainda $\sigma(a_j \alpha^j) = a_j \beta^j$ pois σ é K -homomorfismo.

Finalmente,

$$\sigma \left(\sum_{j=0}^{n-1} a_j \alpha^j \right) = \sum_{j=0}^{n-1} a_j \beta^j = \varphi \left(\sum_{j=0}^{n-1} a_j \alpha^j \right).$$



□

Chamamos de *fecho algébrico* de $\mathbb{Q}$, o conjunto $\overline{\mathbb{Q}}$ de todos os números complexos, algébricos sobre $\mathbb{Q}$. Visto que dados $\alpha, \beta \in \overline{\mathbb{Q}}$ então $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é finito e β também é algébrico sobre $\mathbb{Q}(\alpha)$ então $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ é finito e, portanto,

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$$

é finito. Daí, $\mathbb{Q}(\alpha, \beta)$ é uma extensão algébrica de $\mathbb{Q}$ e $\alpha \pm \beta, \alpha\beta, \alpha^{-1}; \alpha \neq 0 \in \mathbb{Q}(\alpha, \beta) \subset \overline{\mathbb{Q}}$. Logo são algébricos e portanto $\overline{\mathbb{Q}}$ é um corpo.

Sabemos que toda extensão de grau finito é uma extensão algébrica e toda extensão finita dos racionais, recebe o nome de *Corpo de Números*.

Dizemos que um corpo K é *algebricamente fechado* se todo polinômio não constante em $K[X]$ admite uma raiz em K .

Admitindo que o corpo dos números complexos é algebricamente fechado, é fácil ver que o fecho algébrico dos racionais é um corpo algebricamente fechado.

Teorema 1.3 [6] *Dado K , um corpo de números, existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$ e θ é chamado de elemento primitivo.*

Demonstração. Visto que K é um corpo de números, K é infinito e como K é obtido de $\mathbb{Q}$ pela adjunção de um número finito de elementos, podemos supor $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$.

Faremos a demonstração por indução sobre n . Se $n = 1$, $K = \mathbb{Q}(\alpha_1)$ e tomemos $\theta = \alpha_1$. Provando que $\mathbb{Q}(\alpha_1, \alpha_2) = \mathbb{Q}(\theta)$ então, por hipótese de indução sobre s , $s \leq n - 1$ temos que

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = \mathbb{Q}(\beta)(\alpha_n) = \mathbb{Q}(\beta, \alpha_n) = \mathbb{Q}(\theta).$$

Assim sendo, podemos supor $n = 2$. Considere $K = \mathbb{Q}(\theta_1, \beta_1)$, $p(X) = \text{irr}(\theta_1, \mathbb{Q})$ e $q(X) = \text{irr}(\beta_1, \mathbb{Q})$. Tomemos as fatorações, em $\mathbb{C}$, de $p(X)$ e $q(X)$:

$$p(X) = (X - \theta_1) \cdots (X - \theta_n) \text{ e}$$

$$q(X) = (X - \beta_1) \cdots (X - \beta_m).$$

Sejam

$$x_{ik} = \frac{\theta_i - \theta_1}{\beta_1 - \beta_k}, \quad i = 1, \dots, n, k = 2, \dots, m.$$

Sendo $\mathbb{Q}$ é infinito, podemos escolher $c \in \mathbb{Q}$; $c \neq x_{ik}, \forall i, k$. Agora seja $\theta = \theta_1 + c\beta_1$ e mostremos que $\mathbb{Q}(\theta) = \mathbb{Q}(\theta_1, \beta_1)$. Observe que θ é uma combinação linear de θ_1 e β_1 com coeficientes em $\mathbb{Q}$, logo $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\theta_1, \beta_1)$. Devemos mostrar que θ_1 e β_1 estão em $\mathbb{Q}(\theta)$, para isto é suficiente provar que $\beta_1 \in \mathbb{Q}(\theta)$, pois $\theta = \theta_1 - c\beta_1$.

Seja $r(X) = p(\theta - cX) \in \mathbb{Q}(\theta)[X]$. Note que β_1 é raiz de $r(X)$, pois

$$r(\beta_1) = p(\theta - c\beta_1) = p(\theta_1) = 0.$$

Entretanto, para que $r(X)$ e $q(X)$ tenham somente uma raiz comum γ , é preciso que γ seja um dos $\beta_1, \dots, \beta_m$ e $\theta - c\beta_1$ seja um dos $\theta_1, \dots, \theta_n$. Mas pela escolha de c , $\gamma = \beta_1$. Seja $h(X) = \text{irr}(\beta_1, \mathbb{Q}(\theta))$. Então $h(X)$ divide $q(X)$ e $r(X)$ e visto que $q(X)$ e $r(X)$ tem exatamente uma raiz comum em $\mathbb{C}$ e todo polinômio irredutível em $\mathbb{C}$ não tem raízes repetidas, tem-se $\partial h = 1$, isto é, $h(X) = X - \beta$, logo $\beta \in \mathbb{Q}(\theta)$. Daí, $\mathbb{Q}(\theta_1, \beta_1) \subseteq \mathbb{Q}(\theta)$ e, portanto, $\mathbb{Q}(\theta) = \mathbb{Q}(\theta_1, \beta_1)$. $\square$

Exemplo 1.4 Seja $K = \mathbb{Q}(i, \sqrt[3]{2})$. Sejam $f(X) = \text{irr}(i, \mathbb{Q}) = X^2 + 1$, $g(X) = \text{irr}(\sqrt[3]{2}, \mathbb{Q}) = X^3 - 2$ e $\alpha_1 = i$, $\alpha_2 = -i$ as raízes de $f(X)$, $\beta_1 = \sqrt[3]{2}$,

$\beta_2 = \xi_3 \sqrt[3]{2}$ e $\beta_3 = \xi_3^2 \sqrt[3]{2}$ as raízes de $g(X)$. Devemos encontrar $c \in \mathbb{Q}$ tais que

$$c \neq \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_k}, k \neq 1 \quad (*)$$

É fácil verificar que $(*)$ vale para todo $c \in \mathbb{Q}^*$. Portanto, $K = \mathbb{Q}(\theta)$, onde $\theta = i + \sqrt[3]{2}$.

Teorema 1.4 [6] *Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau n . Então existem exatamente n monomorfismos distintos $\sigma_1, \dots, \sigma_n$ de K em $\mathbb{C}$. Se $\theta = \theta_1, \dots, \theta_n$ são todas as raízes de $\text{irr}(\theta, \mathbb{Q})$ então $\sigma_i(\theta) = \theta_i$, determina completamente os monomorfismos σ_i .*

Demonstração. Seja $f(X) = \text{irr}(\theta, \mathbb{Q})$. Pela Proposição 1.4, existe um único isomorfismo $\sigma_i : \mathbb{Q}(\theta) \rightarrow \mathbb{Q}(\theta_i)$, $i = 1, \dots, n$ tal que $\sigma_i(\theta) = \theta_i$. Por outro lado, se existe um monomorfismo $\sigma : K \rightarrow \mathbb{C}$ precisamos mostrar que $\sigma(\theta)$ é raiz de $f(X)$. Visto que

$$0 = \sigma \left(\sum_{i=0}^n a_i \theta^i \right) = f(\sigma(\theta))$$

então $\sigma(\theta)$ é raiz de $f(X)$. Logo $\sigma = \sigma_i$ para algum i e portanto os monomorfismos descritos são os únicos possíveis. $\square$

Sejam $K = \mathbb{Q}(\theta)$, um corpo de números de grau n e $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$. Para cada $\alpha \in K$, definimos o *polinômio característico* de α sobre $\mathbb{Q}$, como sendo

$$f_\alpha(X) = \prod_{i=1}^n (X - \sigma_i(\alpha)).$$

Podemos também escrever

$$f_\alpha(X) = X^n - \left(\sum_{i=1}^n \sigma_i(\alpha) \right) X^{n-1} + \dots + (-1)^n \prod_{i=1}^n \sigma_i(\alpha).$$

Por outro lado,

$$\text{irr}(\alpha, \mathbb{Q}) = \prod_{i=1}^m (X - \alpha_i);$$

sendo α_i as raízes de $\text{irr}(\alpha, \mathbb{Q})$, $i = 1, \dots, m$.

Sejam $\tau_1, \dots, \tau_m$ os monomorfismos de $\mathbb{Q}(\alpha)$ em $\mathbb{C}$ definidos de modo que

$$\alpha_i = \tau_i(\alpha), i = 1, \dots, m.$$

Visto que cada τ_i tem $[K : \mathbb{Q}(\alpha)]$ extensões de K em $\mathbb{C}$, conclui-se que

$$f_\alpha(X) = \text{irr}(\alpha, \mathbb{Q})^{[K : \mathbb{Q}(\alpha)]},$$

consequentemente, os coeficientes de $f_\alpha(X)$ e, em particular, $\sum_{i=1}^n \sigma_i(\alpha)$ e $\prod_{i=1}^n \sigma_i(\alpha)$ são números racionais.

Definição 1.3 *Sejam K um corpo de números de grau n e $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$ e α um elemento de K . Os elementos $\sigma_i(\alpha)$; são chamados de K -conjugados de α .*

Sobre $\mathbb{Q}$, $\sqrt{2}$ e $-\sqrt{2}$ são conjugados. Por outro lado, $1 + \sqrt{3}$ e $\sqrt{3}$ não são $\mathbb{Q}$ -conjugados.

Sejam K um corpo de números de grau n , $\alpha_1, \dots, \alpha_n$ elementos de K e $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$. O *Discriminante* da n -upla $(\alpha_1, \dots, \alpha_n)$ é definido por

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

Exemplo 1.5 *Sejam $K = \mathbb{Q}(\sqrt{7})$ um corpo de números e $\{1, \sqrt{7}\} \subset K$. Então $\Delta[1, \sqrt{7}] = 28$.*



Lema 1.1 *Sejam K um corpo de números de grau n . $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ subconjuntos de K tais que $\beta_k = \sum_{i=1}^n c_{ik} \alpha_i$, com $c_{ik} \in \mathbb{Q}$, $k = 1, \dots, n$. Então*

$$\Delta[\beta_1, \dots, \beta_n] = (\det(c_{ik}))^2 \cdot \Delta[\alpha_1, \dots, \alpha_n].$$

Demonstração. Pela definição

$$\begin{aligned} \Delta[\beta_1, \dots, \beta_n] &= \left(\det \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix} \right)^2 \\ &= \left(\det \begin{pmatrix} \sum_{i=1}^n c_{i1} \sigma_1(\alpha_i) & \cdots & \sum_{i=1}^n c_{in} \sigma_1(\alpha_i) \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n c_{i1} \sigma_n(\alpha_i) & \cdots & \sum_{i=1}^n c_{in} \sigma_n(\alpha_i) \end{pmatrix} \right)^2 \\ &= \left(\det \begin{pmatrix} \sum_{i=1}^n c_{i1} \sigma_1(\alpha_i) & \cdots & \sum_{i=1}^n c_{i1} \sigma_n(\alpha_i) \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^n c_{in} \sigma_1(\alpha_i) & \cdots & \sum_{i=1}^n c_{in} \sigma_n(\alpha_i) \end{pmatrix} \right)^2 \\ &= (\det(c_{ik}))^2 (\det(\sigma_j(\alpha_i)))^2 \\ &= (\det(c_{ik}))^2 \Delta[\alpha_1, \dots, \alpha_n]. \end{aligned}$$

□

Exemplo 1.6 *Já vimos que o discriminante da base $\{1, \sqrt{7}\}$ do corpo de números $K = \mathbb{Q}(\sqrt{7})$ é 28. Agora considerando uma outra base de K , por exemplo $\{2 - \sqrt{7}, 5 + 2\sqrt{7}\}$, segue do Lema 1.1, que*

$$\Delta[2 - \sqrt{7}, 5 + 2\sqrt{7}] = \left(\det \begin{pmatrix} 2 & -1 \\ 5 & 2 \end{pmatrix} \right)^2 \Delta[1, \sqrt{7}] = 9^2 28.$$

Teorema 1.5 [6] *Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau n . Então o discriminante de qualquer base de K é um número racional não nulo.*

Demonstração. Seja $\{1, \theta, \dots, \theta^{n-1}\}$ uma base de K e suponhamos que os conjugados de θ sejam $\theta_1, \dots, \theta_n$. Pela definição de discriminante,

$$\Delta = \Delta[1, \theta, \dots, \theta^{n-1}] = (\det(\theta_i^j))^2.$$

Visto que neste caso $(\det(\theta_i^j))^2$ é um determinante de Vandermonde, temos

$$\Delta = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2$$

e $\Delta \neq 0$ pois $\theta_i \neq \theta_j$ se $i \neq j$.

Sendo $f(X) = \text{irr}(\theta, \mathbb{Q})$ então $f(X) = \prod_{i=1}^n (X - \theta_i)$ e sua derivada $f'(X) = \sum_{i=1}^n \frac{f(X)}{X - \theta_i}$. Calculando a derivada de cada θ_i , temos

$$\pm \prod_{i=1}^n f'(\theta_i) = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2.$$

Mas, $f'(\theta_i) = \sigma_i(f'(\theta))$ e $f'(\theta) \in \mathbb{Q}(\theta)$. Logo o polinômio característico de $f'(\theta)$ sobre $\mathbb{Q}$ é

$$\begin{aligned} f_{f'(\theta)}(X) &= \prod_{i=1}^n (X - \sigma_i(f'(\theta))) \\ &= X^n - \left(\sum_{i=1}^n \sigma_i(f'(\theta)) \right) X^{n-1} + \dots + (-1)^n \prod_{i=1}^n \sigma_i(f'(\theta)). \end{aligned}$$

Visto que cada coeficiente de $f_{f'(\theta)}(X)$ é racional, segue que Δ é um número racional. $\square$

Denotamos por $\bar{\mathbb{Z}}$ o conjunto de todos os números complexos, que são inteiros algébricos, isto é, os números complexos que são raízes de polinômios mônicos com coeficientes inteiros.

Teorema 1.6 [6] *Seja θ uma raiz de um polinômio mônico, com coeficientes inteiros algébricos. Então θ é um inteiro algébrico.*

Demonstração. Seja $\theta^n + a_{n-1}\theta^{n-1} + \dots + a_1\theta + a_0 = 0$, com $a_i \in \overline{\mathbb{Z}}$, $i = 0, \dots, n-1$. Fazendo $A = \mathbb{Z}[a_0, \dots, a_{n-1}, \theta]$ e $b_0 = a_0, \dots, b_{n-1} = a_{n-1}$ e $b_n = \theta$ segue pela Proposição 1.1, $\mathbb{Z}[b_0, \dots, b_n]$ é um $\mathbb{Z}$ -módulo finitamente gerado e portanto θ é um inteiro algébrico. $\square$

Chamamos o conjunto $K \cap \overline{\mathbb{Z}}$ de *Anel dos Inteiros Algébricos* do corpo de números K e denotamos por $\mathcal{O}_K$.

Lema 1.2 [6] *Sejam K um corpo de números e α um elemento de K . Então, para algum $c \in \mathbb{Z}^*$, temos $c\alpha \in \mathcal{O}_K$.*

Demonstração. Seja

$$f(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = \text{irr}(\alpha, \mathbb{Q}).$$

Então existe $c \in \mathbb{Z}^*$ tal que

$$cf(X) = cX^n + ca_{n-1}X^{n-1} + \dots + ca_0 \in \mathbb{Z}[X].$$

Multiplicando $cf(X)$ por c^{n-1} , obtemos o polinômio

$$g(X) = c^n f(X) = (cX)^n + ca_{n-1}(cX)^{n-1} + \dots + c^n a_0 \in \mathbb{Z}[X]$$

que tem α como raiz. Entretanto, substituindo Y por cX , obtemos o polinômio mônico

$$h(Y) = Y^n + ca_{n-1}Y^{n-1} + \dots + c^n a_0,$$

cujos coeficientes são inteiros e tem $c\alpha$ como raiz. Logo $c\alpha \in \mathcal{O}_K$. $\square$

Corolário 1.2 [6] *Seja K um corpo de números, então existe um inteiro algébrico θ tal que $K = \mathbb{Q}(\theta)$.*



Lema 1.3 [6] *Um número algébrico α é um inteiro algébrico se, e somente se seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.*

Demonstração. Seja $p(X) = \text{irr}(\alpha, \mathbb{Q})$. Caso $p(X) \in \mathbb{Z}[X]$ então α é um inteiro algébrico. Reciprocamente, se α é um inteiro algébrico, então existe $q(X) \in \mathbb{Z}[X]$, mônico tal que $q(\alpha) = 0$. Sendo $p(X) = \text{irr}(\alpha, \mathbb{Q})$ e $q(\alpha) = 0$, então $p(X)$ divide $q(X)$, ou seja, $q(X) = p(X)h(X)$ e pelo Lema de Gauss, existe $\lambda \in \mathbb{Q}^*$ de modo que $\lambda p(X)$ e $\lambda^{-1}h(X) \in \mathbb{Z}[X]$. Como $\lambda p(X) \in \mathbb{Z}[X]$ tem-se que $\lambda \in \mathbb{Z}$, pois $p(X)$ é mônico. Analogamente, $\lambda^{-1}h(X) \in \mathbb{Z}[X]$, implicando que $\lambda^{-1} \in \mathbb{Z}$, logo $\lambda = \pm 1$ e, sem perda de generalidade, podemos supor $\lambda = 1$. Portanto $p(X) \in \mathbb{Z}[X]$. $\square$

Lema 1.4 [6] *Um inteiro algébrico é um número racional se, e somente se é um inteiro, isto é, $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

Demonstração. Visto que todo inteiro n é raiz do polinômio $X - n \in \mathbb{Z}[X]$, então n é um inteiro algébrico e portanto $\mathbb{Z} \subseteq \overline{\mathbb{Z}} \cap \mathbb{Q}$. Reciprocamente, se $\alpha \in \overline{\mathbb{Z}} \cap \mathbb{Q}$, então $\alpha \in \overline{\mathbb{Z}}$ e $\alpha \in \mathbb{Q}$. Desde que $\alpha \in \mathbb{Q}$ seu polinômio irredutível sobre $\mathbb{Q}$ é $X - \alpha$ e pelo Lema 1.3 os coeficientes de $X - \alpha$ estão em $\mathbb{Z}$, logo $\alpha \in \mathbb{Z}$ e $\overline{\mathbb{Z}} \cap \mathbb{Q} \subseteq \mathbb{Z}$. Portanto $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. $\square$

1.3 Base Integral

Sejam $K = \mathbb{Q}(\theta)$ um corpo de números de grau n , θ um inteiro algébrico. Mostraremos a seguir que o anel $\mathcal{O}_K$ dos inteiros algébricos de K é um $\mathbb{Z}$ -módulo livre de posto n , ou seja, admite uma base a qual denominamos base integral. Assim, $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral se, e somente se, todo α_i é um inteiro algébrico e cada elemento de $\mathcal{O}_K$ é expressado, de modo único,

como

$$a_1\alpha_1 + \cdots + a_n\alpha_n,$$

com $a_i \in \mathbb{Z}$. Vale observar que $\{1, \theta, \dots, \theta^{n-1}\}$ é uma $\mathbb{Q}$ -base de K , constituída de inteiros algébricos, mas nem sempre é uma base integral de $\mathcal{O}_K$. Por exemplo $\{1, 2\sqrt{2}\}$ é uma $\mathbb{Q}$ -base de $\mathbb{Q}(\sqrt{2})$, mas não é uma base integral.

Lema 1.5 [6] *Se $\{\alpha_1, \dots, \alpha_n\}$ é uma base de K constituída de inteiros algébricos, então o discriminante $\Delta[\alpha_1, \dots, \alpha_n]$ é um inteiro não nulo.*

Demonstração. Pelo Teorema 1.5, $\Delta = \Delta[\alpha_1, \dots, \alpha_n]$ é racional e não nulo. Visto que os α_i são inteiros algébricos seus conjugados também são inteiros algébricos, logo Δ é um inteiro algébrico. Pelo Lema 1.4, Δ é um inteiro. $\square$

Teorema 1.7 [6] *Dado um corpo de números K de grau n , o seu anel de inteiros algébricos $\mathcal{O}_K$ é um $\mathbb{Z}$ -módulo livre de posto n .*

Demonstração. Seja $\{w_1, \dots, w_n\}$ uma base de K , com $w_i \in \mathcal{O}_K$, de modo que $|\Delta[w_1, \dots, w_n]|$ seja mínimo. Suponhamos que $\{w_1, \dots, w_n\}$ não seja base integral. Então existe $w \in \mathcal{O}_K$ tal que

$$w = a_1w_1 + \cdots + a_nw_n,$$

com $a_i \in \mathbb{Q}$, mas nem todos em $\mathbb{Z}$. Sem perda de generalidade, podemos supor $a_1 \notin \mathbb{Z}$. Então $a_1 = a + r$, onde $a \in \mathbb{Z}$ e $0 < r < 1$. Seja

$$\Psi_1 = w - aw_1 = rw_1 + \cdots + a_nw_n,$$

$\Psi_i = w_i; i = 2, \dots, n$. Então $\{\Psi_1, \dots, \Psi_n\}$ é uma base constituída de inteiros algébricos e seu discriminante,

$$\begin{aligned} \Delta[\Psi_1, \dots, \Psi_n] &= \\ &= \left(\det \begin{pmatrix} r & a_2 & \dots & a_n \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \right)^2 \cdot \Delta[w_1, \dots, w_n] = r^2 \Delta[w_1, \dots, w_n]. \end{aligned}$$

Visto que $0 < r < 1$ então $|\Delta[\Psi_1, \dots, \Psi_n]| < |\Delta[w_1, \dots, w_n]|$, contradizendo a minimalidade de $|\Delta[w_1, \dots, w_n]|$. Logo $\{w_1, \dots, w_n\}$ é uma base integral de $\mathcal{O}_K$ e, portanto, $\mathcal{O}_K$ é um $\mathbb{Z}$ -módulo livre de posto n . $\square$

Teorema 1.8 [6] *Sejam K um corpo de números e $\alpha_1, \dots, \alpha_n$ elementos de $\mathcal{O}_K$. Se $\Delta[\alpha_1, \dots, \alpha_n]$ é um inteiro livre de quadrados então $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral.*

Demonstração. Seja $\{\beta_1, \dots, \beta_n\}$ uma base integral. Então existem $c_{ij} \in \mathbb{Z}$ tais que $\alpha_i = \sum c_{ij} \beta_j$ e, pelo Lema 1.1,

$$\Delta = \Delta[\alpha_1, \dots, \alpha_n] = (\det c_{ij})^2 \cdot \Delta[\beta_1, \dots, \beta_n].$$

Sendo Δ um inteiro livre de quadrados, então $\det c_{ij} = \pm 1$ e a matriz (c_{ij}) é inversível. Seja $(d_{ij}) = (c_{ij})^{-1}$; com $d_{ij} \in \mathbb{Z}$. Assim, $\beta_j = \sum d_{ij} \alpha_i$, ou seja, cada $\beta_j \in \mathcal{O}_K$ se escreve como combinação linear, a coeficientes inteiros, dos α_i . Portanto $\{\alpha_1, \dots, \alpha_n\}$ é uma base integral. $\square$

Exemplo 1.7 A $\mathbb{Q}$ -base $\{1, \frac{1}{2} + \frac{\sqrt{17}}{2}\}$ de $\mathbb{Q}(\sqrt{17})$ é constituída de inteiros algébricos e tem discriminante 17. Pelo Teorema 1.8, segue que $\{1, \frac{1}{2} + \frac{\sqrt{17}}{2}\}$ é uma base integral.

Observação 1.2 $\{\alpha_1, \dots, \alpha_n\}$ ser base integral não implica que $\Delta[\alpha_1, \dots, \alpha_n]$ seja um inteiro livre de quadrados.

Lema 1.6 Seja K um corpo de números de grau n e $\mathcal{O}_K$ o seu anel de inteiros algébricos. Se $\{\alpha_1, \dots, \alpha_n\}$ e $\{\beta_1, \dots, \beta_n\}$ são duas bases integrais de $\mathcal{O}_K$ então

$$\Delta[\alpha_1, \dots, \alpha_n] = \Delta[\beta_1, \dots, \beta_n].$$

Demonstração. Visto que existe uma matriz C inversível, com entradas inteiras tal que $\alpha_i = \sum c_{ij}\beta_j$ então, pelo Lema 1.1,

$$\Delta[\alpha_1, \dots, \alpha_n] = (\det C)^2 \Delta[\beta_1, \dots, \beta_n] = \Delta[\beta_1, \dots, \beta_n]$$

pois, a matriz de mudança de base C é unimodular. □

Pelo Lema 1.6, podemos definir o discriminante de um corpo de números K como sendo o discriminante de alguma base integral de $\mathcal{O}_K$ e denotamos por $\mathfrak{D}_K$.

1.4 Norma e Traço

Sejam $K \subset L$ corpos de números, $[L : K] = n$, $\sigma_1, \dots, \sigma_n$ os K -monomorfismos de L em $\mathbb{C}$ e $\alpha \in L$. Definimos a norma e o traço de α relativamente a L e K , como sendo

$$\prod_{i=1}^n \sigma_i(\alpha) \quad \text{e} \quad \sum_{i=1}^n \sigma_i(\alpha),$$

os quais serão denotados por $N_{L|K}(\alpha)$ e $Tr_{L|K}(\alpha)$, respectivamente.

Sejam $K \subset L \subset M$ corpos de números, $\alpha, \beta \in M$ e $a \in K$. Então valem as seguintes propriedades:

1. $N_{M/K}(\alpha\beta) = N_{M/K}(\alpha)N_{M/K}(\beta),$
2. $Tr_{M/K}(\alpha + \beta) = Tr_{M/K}(\alpha) + Tr_{M/K}(\beta),$
3. $Tr_{M/K}(a\alpha) = aTr_{M/K}(\alpha),$
4. $Tr_{M/K}(a) = [M : K]a,$
5. $N_{M/K}(a) = a^{[M:K]},$
6. $N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)),$
7. $Tr_{M/K}(\alpha) = Tr_{L/K}(Tr_{M/L}(\alpha)).$

Proposição 1.5 [6] *Sejam $K = \mathbb{Q}(\theta)$ um corpo de números de grau n e $f(X) = \text{irr}(\theta, \mathbb{Q})$. Então*

$$\Delta[1, \theta, \dots, \theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta)),$$

com $f'(X)$ sendo a derivada formal de $f(X)$.

Demonstração. Pelo Teorema 1.5, temos

$$\left(\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) \right)^2 = (-1)^s \prod_{i=1}^n f'(\theta_i),$$

com $s = \frac{1}{2}n(n-1)$. Mas,

$$\prod_{i=1}^n f'(\theta_i) = \prod_{i=1}^n f'(\sigma_i(\theta)) = \prod_{i=1}^n \sigma_i(f'(\theta)) = N_{K/\mathbb{Q}}(f'(\theta)),$$

então

$$N_{K/\mathbb{Q}}(f'(\theta)) = (-1)^{\frac{n(n-1)}{2}} \left(\prod_{1 \leq i < k \leq n} (\theta_i - \theta_k) \right)^2$$

e, consequentemente,

$$\left(\prod_{1 \leq i < k \leq n} (\theta_i - \theta_k) \right)^2 = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta)).$$

Portanto

$$\Delta[1, \theta, \dots, \theta^{n-1}] = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta)).$$

□

Exemplo 1.8 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$ e $f(X) = X^3 - 2 = \text{irr}(\theta, \mathbb{Q})$. Então $\Delta[1, \theta, \theta^2] = (-1)^3 N_{K/\mathbb{Q}}(f'(3\theta^2)) = -(3\theta^2)^3 = -27.4$.

1.5 Fatoração de Ideais

A fatoração de um número depende do anel em que este é considerado como elemento. Por exemplo, o número 18 no anel dos inteiros algébricos $\mathbb{Z}[\sqrt{-17}]$ de $\mathbb{Q}(\sqrt{-17})$ têm as seguintes fatorações:

$$18 = 2 \cdot 3 \cdot 3$$

$$18 = (1 + \sqrt{-17})(1 - \sqrt{-17})$$

Verifica-se que 2, 3, $1 + \sqrt{-17}$ e $1 - \sqrt{-17}$ são irredutíveis em $\mathbb{Z}[\sqrt{-17}]$, através do cálculo de suas normas. Logo temos duas fatorações distintas de elementos irredutíveis para o número 18 no anel $\mathbb{Z}[\sqrt{-17}]$ e, portanto, concluímos que neste anel a fatoração não é única.

Uma forma alternativa desenvolvida por Kummer e Dedekind, foi procurar estabelecer fatoração única de ideais e isto foi obtido no anel dos inteiros algébricos de um corpo de números.

Os principais objetivos desta Seção são provar que o anel dos inteiros algébricos de um corpo de números é um Domínio de Dedekind e mostrar a unicidade da fatoração de um ideal não nulo como um produto de ideais primos neste domínio.

Um A -módulo M é dito Noetheriano se satisfaz uma das seguintes condições equivalentes:



1. Toda família não vazia de submódulos de M tem um elemento maximal.
2. Toda sequência crescente de submódulos de M é estacionária.
3. Todo submódulo de M é finitamente gerado.

Teorema 1.9 [6] *O anel dos inteiros algébricos $\mathcal{O}_K$ de um corpo de números K , satisfaz as seguintes propriedades:*

1. $\mathcal{O}_K$ é um domínio, com o corpo de frações K .
2. $\mathcal{O}_K$ é Noetheriano.
3. $\mathcal{O}_K$ é integralmente fechado.
4. Todo ideal primo não nulo de $\mathcal{O}_K$ é maximal.

Demonstração. (1) Denotemos por $Fr(\mathcal{O}_K)$ o corpo de frações de $\mathcal{O}_K$. Claramente $Fr(\mathcal{O}_K) \subset K$ pois, $\mathcal{O}_K \subset K$. Por outro lado, $K \subset Fr(\mathcal{O}_K)$ pois, dado $\alpha \in K$, pelo Lema 1.2, $c\alpha \in \mathcal{O}_K$, com $c \in \mathbb{Z}^*$, assim $\frac{c\alpha}{c} \in Fr(\mathcal{O}_K)$ e, portanto, $K = Fr(\mathcal{O}_K)$.

(2) Sabemos que $\mathcal{O}_K$ é um $\mathbb{Z}$ -módulo livre de posto n e sendo $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$ então $\mathfrak{a}$ é um submódulo livre de posto $\leq n$. Logo admite uma base finita e portanto $\mathfrak{a}$ é finitamente gerado. Logo $\mathcal{O}_K$ é Noetheriano.

(3) Segue imediatamente do Teorema 1.6.

(4) Sejam $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e $\alpha \neq 0$, $\alpha \in \mathfrak{p}$. Então

$$N(\alpha) = \alpha_1 \dots \alpha_n = s,$$

sendo α_i são os conjugados de α , com $\alpha_1 = \alpha$. Visto que $\alpha_1 \in \mathfrak{p}$ então $s \in \mathfrak{p}$ e daí, $\langle s \rangle \subset \mathfrak{p}$. Tendo $\langle s \rangle \subset \mathfrak{p}$ implica que

$$\#(\frac{\mathcal{O}_K}{\langle s \rangle}) > \#(\frac{\mathcal{O}_K}{\mathfrak{p}}),$$

então precisamos mostrar que o anel quociente $\frac{\mathcal{O}_K}{\mathfrak{p}}$ é finito. Logo é suficiente provar que o anel quociente $\frac{\mathcal{O}_K}{(s)}$ é finito. Sejam $\{e_1, \dots, e_m\}$ uma base integral de $\mathcal{O}_K$ e

$$X = \{a_1 e_1 + \dots + a_m e_m; a_i \in \mathbb{Z}, 0 \leq a_i < s\}$$

assim $\#X = m^s$. Dado $x \in \mathcal{O}_K$, $x = \sum_{i=1}^m b_i e_i$, $b_i \in \mathbb{Z}$. Mas

$$x = s \sum_{i=1}^m q_i e_i + \sum_{i=1}^m r_i e_i;$$

onde $0 \leq r_i < b_i$, e como $s \in \mathfrak{p}$ e $q_i e_i \in \mathcal{O}_K$, segue que $s q_i e_i \in \mathfrak{p}$ e

$$\bar{x} = \overline{\sum_{i=1}^m r_i e_i}.$$

Portanto $\frac{\mathcal{O}_K}{(s)}$ é finito. Entretanto, sendo que $\mathfrak{p}$ é um ideal primo, $\frac{\mathcal{O}_K}{\mathfrak{p}}$ é um domínio e como é finito, $\frac{\mathcal{O}_K}{\mathfrak{p}}$ é um corpo. Portanto $\mathfrak{p}$ é um ideal maximal. $\square$

Quando um anel satisfaz todas as condições do Teorema 1.9 é chamado *Domínio de Dedekind*.

Dados $\mathfrak{a}$ e $\mathfrak{b}$ ideais de $\mathcal{O}_K$, definimos o produto de $\mathfrak{a}$ por $\mathfrak{b}$ (e indicamos por $\mathfrak{a}\mathfrak{b}$) como sendo o conjunto de todas as somas da forma $\sum_{i=1}^n a_i b_i$, com $a_i \in \mathfrak{a}$ e $b_i \in \mathfrak{b}$. O produto $\mathfrak{a}\mathfrak{b}$ é também um ideal de $\mathcal{O}_K$, e vale a inclusão $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Dizemos que $\mathfrak{a}$ divide $\mathfrak{b}$ se $\mathfrak{b} \subset \mathfrak{a}$ e denotamos essa relação por $\mathfrak{a} \mid \mathfrak{b}$.

Definição 1.4 Seja $\mathcal{O}_K$ o anel dos inteiros algébricos de um corpo de números K . Dizemos que um $\mathcal{O}_K$ -submódulo $\mathfrak{a}$ de K é um ideal fracionário de $\mathcal{O}_K$ se existir um elemento c não nulo de $\mathcal{O}_K$ tal que $c\mathfrak{a}$ é um ideal de $\mathcal{O}_K$.

A soma, o produto e a interseção de dois ideais fracionários de $\mathcal{O}_K$ se define de forma análoga ao produto de ideais ordinários e $\mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{a}_1 \cdot \mathfrak{a}_2$ e $\mathfrak{a}_1 \cap \mathfrak{a}_2$ são também ideais fracionários de $\mathcal{O}_K$.

Os dois Teoremas abaixo enunciados representam os principais resultados desta seção e serão demonstrados juntos, em uma série de etapas.

Teorema 1.10 [6] *O conjunto dos ideais fracionários não nulos de $\mathcal{O}_K$ formam um grupo abeliano multiplicativo.*

Teorema 1.11 [6] *Todo ideal não nulo de $\mathcal{O}_K$ pode ser escrito como um produto de ideais primos, unicamente a menos da ordem dos fatores.*

Demonstração. 1. Seja $\mathfrak{a} \neq 0$ um ideal de $\mathcal{O}_K$. Então existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ tais que $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Sejam $\mathfrak{a} \subset \mathcal{O}_K$, $\mathfrak{a} \neq 0$, $r \in \mathbb{N}^*$, $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ ideais primos tais que

$$\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq \mathfrak{a} \quad (*).$$

Seja $\Phi = \{\mathfrak{a} : \text{ideal}, \mathfrak{a} \subset \mathcal{O}_K \text{ tal que não satisfaz } (*)\}$. Suponhamos $\Phi \neq \emptyset$. Sendo $\mathcal{O}_K$ Noetheriano então existe $\mathfrak{b} \in \Phi$ tal que $\mathfrak{b}$ é o elemento maximal de Φ . Tal ideal $\mathfrak{b}$ não é primo e $\mathfrak{b} \neq \mathcal{O}_K$. Assim existem ideais $\mathfrak{d}, \mathfrak{c}$ de $\mathcal{O}_K$, com $\mathfrak{d}, \mathfrak{c} \subseteq \mathfrak{b}$, $\mathfrak{d} \not\subseteq \mathfrak{b}$, $\mathfrak{c} \not\subseteq \mathfrak{b}$.

Sejam

$$\mathfrak{a}_1 = \mathfrak{b} + \mathfrak{d} \quad \text{e} \quad \mathfrak{a}_2 = \mathfrak{b} + \mathfrak{c}.$$

Então

$$\mathfrak{a}_1 \mathfrak{a}_2 = (\mathfrak{b} + \mathfrak{d})(\mathfrak{b} + \mathfrak{c}) \subseteq \mathfrak{b}, \mathfrak{a}_1 \not\subseteq \mathfrak{b}, \mathfrak{a}_2 \not\subseteq \mathfrak{b}$$

e pela maximalidade de $\mathfrak{b}$ existem ideais primos $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{p}_{s+1}, \dots, \mathfrak{p}_r$ tais que

$$\mathfrak{p}_1, \dots, \mathfrak{p}_s \subseteq \mathfrak{a}_1,$$

$$\mathfrak{p}_{s+1}, \dots, \mathfrak{p}_r \subseteq \mathfrak{a}_2.$$

Logo,

$$\mathfrak{p}_1, \dots, \mathfrak{p}_r \subseteq \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{b}$$

o que contraria a escolha de $\mathfrak{b}$. Portanto $\Phi = \emptyset$. Visto que $\mathfrak{a} \neq 0$ concluímos que $\mathfrak{p}_i \neq 0$, para qualquer $i = 1, \dots, r$.

2. Definição de como funciona o inverso de um ideal $\mathfrak{a}$ de $\mathcal{O}_K$.

Para cada ideal $\mathfrak{a}$ de $\mathcal{O}_K$,

$$\mathfrak{a}^{-1} = \{x \in K; x\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

Afirmção 1. $\mathfrak{a}^{-1}$ é um $\mathcal{O}_K$ -submódulo. De fato: (i) Sejam $n_1, n_2 \in \mathfrak{a}^{-1}$, ou seja, $n_1 \in K$ tal que $n_1\mathfrak{a} \subseteq \mathcal{O}_K$ e $n_2 \in K$ tal que $n_2\mathfrak{a} \subseteq \mathcal{O}_K$. Então

$$(n_1 + n_2)\mathfrak{a} = n_1\mathfrak{a} + n_2\mathfrak{a} \subseteq \mathcal{O}_K.$$

(ii) Para qualquer $\alpha \in \mathcal{O}_K$, $\alpha \in K$, pois $\mathcal{O}_K \subset K$ e dado $x \in \mathfrak{a}^{-1}$ tem-se que $x \in K$ e $x\mathfrak{a} \subseteq \mathcal{O}_K$, logo $(\alpha x)\mathfrak{a} = \alpha(x\mathfrak{a}) \subseteq \mathcal{O}_K$ o que implica $\alpha x \in \mathfrak{a}^{-1}$.

Afirmção 2. $\mathfrak{a}^{-1}$ é um ideal fracionário. De fato, se $\mathfrak{a} \neq 0$ então para algum $c \in \mathfrak{a}$, $c \neq 0$, temos $c\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$.

Afirmção 3. $\mathcal{O}_K \subseteq \mathfrak{a}^{-1}$. De fato, dado $x \in \mathcal{O}_K$ temos que $x\mathfrak{a} \subseteq \mathfrak{a} \subseteq \mathcal{O}_K$, logo $x \in \mathfrak{a}^{-1}$. Portanto $\mathcal{O}_K \subseteq \mathfrak{a}^{-1}$. Pela afirmação 3, $\mathfrak{a} = \mathfrak{a}\mathcal{O}_K \subseteq \mathfrak{a}\mathfrak{a}^{-1}$ e da definição de $\mathfrak{a}^{-1}$, $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{a}^{-1}\mathfrak{a} \subseteq \mathcal{O}_K$. De fato, dado $x \in \mathfrak{a}^{-1}$, $x\mathfrak{a} \subseteq \mathcal{O}_K$ e $y \in \mathfrak{a}$ então

$$(x\mathfrak{a}) = x(\mathfrak{a}y) = x\mathfrak{a} \subseteq \mathcal{O}_K.$$

Portanto $\mathfrak{a}\mathfrak{a}^{-1}$ é um ideal de $\mathcal{O}_K$.

Observe que dados $\mathfrak{p}, \mathfrak{a}$ ideais de $\mathcal{O}_K$, $\mathfrak{a} \subseteq \mathfrak{p}$ implica que $\mathcal{O}_K \subseteq \mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$.

3. Se $\mathfrak{a}$ é um ideal próprio, então $\mathcal{O}_K \subsetneq \mathfrak{a}^{-1}$.

Sendo $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{p}$ ideal maximal então $\mathfrak{p}^{-1} \subseteq \mathfrak{a}^{-1}$ e assim é suficiente provar que $\mathfrak{p}^{-1} \neq \mathcal{O}_K$. Seja $a \in \mathfrak{p}$, $a \neq 0$. Pelo item 2, podemos considerar o menor



r tal que

$$p_1, \dots, p_r \subseteq \langle a \rangle,$$

para $p_1, \dots, p_r$ primos. Visto que $\langle a \rangle \subseteq p$ e p é primo então algum $p_i \subseteq p$. Suponhamos sem perda de generalidade $p_1 \subseteq p$. Daí $p_1 = p$ e p é maximal. Logo $p_2 \dots p_r \not\subseteq \langle a \rangle$ pela minimalidade de r . Portanto existe $b \in p_2 \dots p_r$ tal que b não pertença à $\langle a \rangle$. mas $bp \subseteq \langle a \rangle$ então $ba^{-1}p \subseteq \mathcal{O}_K$ e pela definição de p^{-1} segue $ba^{-1} \in p^{-1}$. Por outro lado $b \notin a\mathcal{O}_K$ então $ba^{-1} \notin \mathcal{O}_K$, logo $p^{-1} \neq \mathcal{O}_K$ e, consequentemente, $a^{-1} \neq \mathcal{O}_K$.

4. Se a é um ideal não nulo e $aS \subseteq a$ para qualquer subconjunto $S \subseteq K$, então $S \subseteq \mathcal{O}_K$.

Devemos mostrar que se $a\alpha \subseteq a$ para $\alpha \in S$, então $\alpha \in \mathcal{O}_K$. Já que $S \subseteq K$, $\alpha \in K$ e pelo Teorema 1.9, $\alpha \in \mathcal{O}_K$. Portanto $S \subseteq \mathcal{O}_K$.

5. Se p é um ideal maximal então $pp^{-1} = \mathcal{O}_K$.

Pelo item 2, pp^{-1} é um ideal com $p \subseteq pp^{-1} \subseteq \mathcal{O}_K$. Visto que p é maximal $pp^{-1} = p$ ou $pp^{-1} = \mathcal{O}_K$. Se $pp^{-1} = p$ então pelo item 4, $p^{-1} \subseteq \mathcal{O}_K$ o que contraria o item 3. Logo $pp^{-1} = \mathcal{O}_K$.

6. Para todo ideal $a \neq 0$, $aa^{-1} = \mathcal{O}_K$.

Seja a maximal tal que $aa^{-1} \neq \mathcal{O}_K$. Então $a \subseteq p$, p maximal e pelo item 2, $\mathcal{O}_K \subseteq p^{-1} \subseteq a^{-1}$, logo

$$a \subseteq ap^{-1} \subseteq aa^{-1} \subseteq \mathcal{O}_K.$$

Em particular ap^{-1} é um ideal de $\mathcal{O}_K$. Deste modo não vale $a = ap^{-1}$, pois implicaria pelo item 4, $p^{-1} \subseteq \mathcal{O}_K$, contradizendo mais uma vez o item 3. Assim, $a \subsetneq ap^{-1}$ e pela maximalidade de a , segue que ap^{-1} satisfaz

$$ap^{-1}(ap^{-1})^{-1} = \mathcal{O}_K$$

e pela definição de $\mathfrak{a}^{-1}$,

$$\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}^{-1}$$

ou

$$\mathfrak{a}\mathfrak{p}^{-1}(\mathfrak{a}\mathfrak{p}^{-1})^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1}.$$

Assim

$$\mathcal{O}_K \subseteq \mathfrak{a}\mathfrak{a}^{-1} \text{ e } \mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathcal{O}_K.$$

7. Todo ideal fracionário $\mathfrak{a}$ tem um inverso $\mathfrak{a}^{-1}$ tal que $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.

Sabemos que o conjunto $\mathfrak{F}$ dos ideais fracionários é um semi-grupo, isto é, vale a lei do fechamento e tem unidade. Então dado um ideal fracionário $\mathfrak{a}$ somente precisamos encontrar outro ideal fracionário $\mathfrak{t}$ tal que $\mathfrak{a}\mathfrak{t} = \mathcal{O}_K$, e neste caso $\mathfrak{t}$ será o inverso. Mas existe um ideal $\mathfrak{b}$ e um elemento $c \neq 0$, $c \in \mathcal{O}_K$ tal que $\mathfrak{a} = c^{-1}\mathfrak{b}$ e considere $\mathfrak{t} = c\mathfrak{b}^{-1}$ então $\mathfrak{a}\mathfrak{t} = \mathcal{O}_K$ e, portanto, o conjunto dos ideais fracionários de $\mathcal{O}_K$ é um grupo abeliano multiplicativo.

8. Todo ideal não nulo $\mathfrak{a}$ é um produto de ideais primos.

Suponhamos $\mathfrak{a}$ maximal e ainda que $\mathfrak{a}$ não se fatore em produto de ideais primos. Logo $\mathfrak{a}$ não é primo, mas $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{p}$ maximal, e pelo item 6, $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathcal{O}_K$. Por outro lado, pela maximalidade de $\mathfrak{a}$ temos que $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$ ou $\mathfrak{a}\mathfrak{p}^{-1} = \mathcal{O}_K$. Logo

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r;$$

$\mathfrak{p}_i$; $i = 2, \dots, r$, ideais primos e, portanto, $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$.

9. A fatoração de ideais é única.

Sejam $\mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s$ ideais primos não nulos tais que

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s.$$

Suponhamos que para todo $t < \min\{r, s\}$, seja verdadeira a seguinte afirmação: Se $\mathfrak{a}_1, \dots, \mathfrak{a}_t, \mathfrak{b}_1, \dots, \mathfrak{b}_s$ são ideais primos não nulos tais que $\mathfrak{a}_1 \cdots \mathfrak{a}_t = \mathfrak{b}_1 \cdots \mathfrak{b}_s$ então $t = s$ e $\mathfrak{a}_i = \mathfrak{b}_i, i = 1, \dots, s$. Se $\min\{r, s\} = 1$, consideremos por exemplo $r = 1$. Então $\mathfrak{a}_1 = \mathfrak{b}_1 \cdots \mathfrak{b}_s$, e como $\mathfrak{a}_1$ é primo tem-se $s = 1$. De $\mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s \subset \mathfrak{q}_1$, tiramos $\mathfrak{q}_1$ divide $\mathfrak{p}_1 \cdots \mathfrak{p}_r$, e sem perda de generalidade podemos supor $\mathfrak{q}_1 = \mathfrak{p}_1$. Obtemos assim

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

O resultado segue da hipótese de indução. Portanto todo ideal de $\mathcal{O}_K$ pode ser fatorado de modo único como produtos de ideais primos. $\square$

Dados $A \subset B$, anéis e $\mathfrak{a} \subset A$ um ideal. Denotamos por $\mathfrak{a}B$ ao ideal de B formado pelos elementos da forma $\sum_{i=1}^n x_i y_i, x_i \in \mathfrak{a}, y_i \in B, i = 1, \dots, n$.

Proposição 1.6 [7] *Sejam $K \subset L$ corpos de números, com $[L : K] = n$, $\mathfrak{p}$ um ideal primo não nulo de $\mathcal{O}_K$ e*

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^q \mathfrak{b}_i^{e_i}$$

a decomposição de $\mathfrak{p}\mathcal{O}_L$ em ideais primos de $\mathcal{O}_L$. Então os $\mathfrak{b}_i$'s são precisamente os ideais primos $\mathfrak{q}$ de $\mathcal{O}_L$ tais que $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$.

Neste caso, dizemos que $\mathfrak{q}$ está acima de $\mathfrak{p}$.

Indicamos por f_i o número $[\frac{\mathcal{O}_L}{\mathfrak{b}_i} : \frac{\mathcal{O}_K}{\mathfrak{p}}]$ e chamamos de *grau residual* de $\mathfrak{b}_i$ sobre $\mathcal{O}_K$. O elemento e_i é chamado de *índice de ramificação* de $\mathfrak{b}_i$ sobre $\mathcal{O}_K$, e se $e_i > 1$ para algum índice i , dizemos que $\mathfrak{p}$ se ramifica em $\mathcal{O}_L$.

Teorema 1.12 [7] *(Igualdade Fundamental) Com as mesmas notações acima temos:*

$$n = \sum_{i=1}^q e_i f_i = [\frac{\mathcal{O}_L}{\mathfrak{p}\mathcal{O}_L} : \frac{\mathcal{O}_K}{\mathfrak{p}}].$$

Teorema 1.13 [7] *Seja K um corpo de números. Uma condição necessária e suficiente para que um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifique em $\mathcal{O}_K$ é que p divida $\mathfrak{D}_K$.*

Em decorrência deste resultado, existe apenas um número finito de primos que se ramifica em $\mathcal{O}_K$.

Lema 1.7 (Lema de Kummer) *Sejam K um corpo de números, $\mathcal{O}_K$ o seu anel de inteiros algébricos e $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Dados um número primo p tal que não divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ e $f(X)$ o polinômio irredutível de θ sobre $\mathbb{Q}$, então existem $p_1(X), \dots, p_q(X) \in \mathbb{Z}[X]$, polinômios irredutíveis, $e_1, \dots, e_q \in \mathbb{N}^*$ tais que $f(X) \equiv p_1(X)^{e_1} \cdots p_q(X)^{e_q} \pmod{p\mathbb{Z}[X]}$ e*

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

1.6 Norma de um Ideal

Nesta Seção definimos a norma de um ideal, como uma generalização de norma de um elemento de $\mathcal{O}_K$ e em seguida mostramos que a função norma é multiplicativa.

Sejam K um corpo de números, $\mathcal{O}_K$ o seu anel de inteiros algébricos e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Definimos a norma de $\mathfrak{a}$ como sendo a cardinalidade do anel quociente $\frac{\mathcal{O}_K}{\mathfrak{a}}$ e denotamos por $N(\mathfrak{a})$.

Em outras palavras,

$$N(\mathfrak{a}) = \#(\frac{\mathcal{O}_K}{\mathfrak{a}}).$$



Teorema 1.14 [6] *Sejam K um corpo de números de grau n e $\mathcal{O}_K$ o seu anel de inteiros algébricos. Então*

1. *Todo ideal $\mathfrak{a}$ não nulo de $\mathcal{O}_K$ tem uma $\mathbb{Z}$ -base $\{\alpha_1, \dots, \alpha_n\}$.*
2. *A norma de um ideal $\mathfrak{a}$ não nulo de $\mathcal{O}_K$ satisfaz*

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \dots, \alpha_n]}{\mathfrak{D}_K} \right|^{\frac{1}{2}}.$$

Demonstração. 1. Pelo Teorema 1.7, $\mathcal{O}_K$ é um $\mathbb{Z}$ -módulo livre de posto n e visto que o anel quociente $\frac{\mathcal{O}_K}{\mathfrak{a}}$ é finito então $\mathfrak{a}$ é um $\mathbb{Z}$ -módulo livre também de posto n , portanto admite uma base $\{\alpha_1, \dots, \alpha_n\}$.

2. Seja $\{w_1, \dots, w_n\}$ uma $\mathbb{Z}$ -base de $\mathcal{O}_K$ e suponhamos $\alpha_i = \sum_{j=1}^n c_{ij} w_j$; $j = 1, \dots, n$.

Visto que $\mathcal{O}_K$ e $\mathfrak{a}$ têm posto n então

$$N(\mathfrak{a}) = \# \left(\frac{\mathcal{O}_K}{\mathfrak{a}} \right) = |\det c_{ij}|.$$

Pelo Lema 1.1,

$$\begin{aligned} \Delta[\alpha_1, \dots, \alpha_n] &= (\det c_{ij})^2 \cdot \Delta[w_1, \dots, w_n] \\ &= (N(\mathfrak{a}))^2 \cdot \mathfrak{D}_K \end{aligned}$$

e a demonstração está concluída. □

Em consequência deste resultado, se $\mathfrak{a} = \langle a \rangle$ é um ideal principal então $N(\mathfrak{a}) = |N(a)|$.

Teorema 1.15 [6] *Sejam K um corpo de números de grau n , $\mathcal{O}_K$ o seu anel de inteiros algébricos e $\mathfrak{a}, \mathfrak{b}$ ideais não nulos de $\mathcal{O}_K$. Então*

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b}).$$



Demonstração. Pela unicidade da fatoração e indução sobre o número de fatores primos é suficiente provar que

$$N(\mathfrak{ap}) = N(\mathfrak{a})N(\mathfrak{p}), \quad (1.1)$$

onde $\mathfrak{p}$ é um ideal primo.

Provemos que

$$\#(\frac{\mathcal{O}_K}{\mathfrak{ap}}) = \#(\frac{\mathcal{O}_K}{\mathfrak{a}}) \cdot \#(\frac{\mathfrak{a}}{\mathfrak{ap}}) \quad (1.2)$$

e

$$\#(\frac{\mathfrak{a}}{\mathfrak{ap}}) = \#(\frac{\mathcal{O}}{\mathfrak{p}}) \quad (1.3)$$

Para provar a Equação (1.2) consideremos o homomorfismo de anéis

$$\begin{aligned} \Phi : \frac{\mathcal{O}_K}{\mathfrak{ap}} &\rightarrow \frac{\mathcal{O}_K}{\mathfrak{a}} \\ \mathfrak{ap} + x &\rightarrow \mathfrak{a} + x. \end{aligned}$$

Observe que Φ está bem definida pois, dados $\mathfrak{ap} + x, \mathfrak{ap} + y \in \frac{\mathcal{O}_K}{\mathfrak{ap}}$, $\Phi(\mathfrak{ap} + x) = \Phi(\mathfrak{ap} + y) \Leftrightarrow \mathfrak{a} + x = \mathfrak{a} + y \Leftrightarrow x - y \in \mathfrak{a}$. A aplicação Φ é sobrejetiva e o $\ker \Phi = \{\mathfrak{ap} + x; x \in \mathfrak{a}\} = \mathfrak{a}/\mathfrak{ap}$. Logo pelo Teorema do Isomorfismo de anéis,

$$\frac{\frac{\mathcal{O}_K}{\mathfrak{ap}}}{\frac{\mathfrak{a}}{\mathfrak{ap}}} \simeq \frac{\mathcal{O}_K}{\mathfrak{a}}$$

e, pelo Teorema de Lagrange,

$$\#(\frac{\mathcal{O}_K}{\mathfrak{ap}}) = \#(\frac{\mathcal{O}_K}{\mathfrak{a}}) \cdot \#(\frac{\mathfrak{a}}{\mathfrak{ap}}).$$

Agora para provar a Equação 1.3, observe que pela fatoração única $\mathfrak{a} \neq \mathfrak{ap}$ implica que $\mathfrak{a} \not\supseteq \mathfrak{ap}$. Mostremos que não existe ideal $\mathfrak{b}$ entre $\mathfrak{a}$ e $\mathfrak{ap}$. De fato

se $\mathfrak{a} \supseteq \mathfrak{b} \supseteq \mathfrak{ap}$ então $\mathfrak{a}^{-1}\mathfrak{a} \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{a}^{-1}\mathfrak{ap}$, ou seja, $\mathcal{O}_K \supseteq \mathfrak{a}^{-1}\mathfrak{b} \supseteq \mathfrak{p}$. Visto que $\mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K$ então $\mathfrak{a}^{-1}\mathfrak{b}$ é um ideal, e sendo $\mathfrak{p}$ maximal, temos $\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_K$ ou $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$, logo $\mathfrak{b} = \mathfrak{a}$ ou $\mathfrak{b} = \mathfrak{ap}$.

Portanto para qualquer elemento $b \in \frac{\mathfrak{a}}{\mathfrak{ap}}$, tem-se

$$\mathfrak{ap} + \langle b \rangle = \mathfrak{a}. \quad (1.4)$$

Fixado um elemento $a \in \frac{\mathfrak{a}}{\mathfrak{ap}}$, definamos a aplicação

$$\begin{aligned} \Psi: \mathcal{O}_K &\rightarrow \frac{\mathfrak{a}}{\mathfrak{ap}} \\ x &\rightarrow \mathfrak{ap} + ax. \end{aligned}$$

A aplicação Ψ é um homomorfismo de $\mathcal{O}_K$ -módulos e sua sobrejetividade decorre da Equação 1.4. Claramente o núcleo da aplicação Ψ é um ideal que satisfaz $\mathfrak{p} \subseteq \ker \Psi$. Desde que $\ker \Psi \neq \mathcal{O}_K$ e $\mathfrak{p}$ maximal então $\ker \Psi = \mathfrak{p}$. Pelo Teorema de Isomorfismo para módulos,

$$\frac{\mathcal{O}_K}{\mathfrak{p}} \simeq \frac{\mathfrak{a}}{\mathfrak{ap}}$$

logo

$$\#(\frac{\mathfrak{a}}{\mathfrak{ap}}) = \#(\frac{\mathcal{O}_K}{\mathfrak{p}})$$

Portanto

$$N(\mathfrak{ap}) = \#(\frac{\mathcal{O}_K}{\mathfrak{ap}}) = \#(\frac{\mathcal{O}_K}{\mathfrak{a}}) \cdot \#(\frac{\mathfrak{a}}{\mathfrak{p}}) = N(\mathfrak{a})N(\mathfrak{p})$$

□

Teorema 1.16 [6] *Sejam K um corpo de números de grau n , $\mathcal{O}_K$ o seu anel de inteiros algébricos e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Então*

1. *Se $N(\mathfrak{a})$ é um primo então $\mathfrak{a}$ é um ideal primo.*

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

Demonstração. (1) Seja $\mathfrak{a} = \prod_{i=1}^n \mathfrak{p}_i^{m_i}$, $\mathfrak{p}_i$ primos, então

$$N(\mathfrak{a}) = \prod_{i=1}^n N(\mathfrak{p}_i)^{m_i}.$$

Logo $N(\mathfrak{a})$ é primo se $n = 1$, $m_1 = 1$ e portanto $\mathfrak{a}$ é primo.

(2) Visto que $N(\mathfrak{a}) = \# \left(\frac{\mathcal{O}_K}{\mathfrak{a}} \right)$ então para qualquer $x \in \mathcal{O}_K$, $N(\mathfrak{a})x \in \mathfrak{a}$, isto é, $N(\mathfrak{a})\bar{x} = \overline{N(\mathfrak{a})x} = \bar{0}$. Fazendo $x = 1$ obtemos $N(\mathfrak{a}) \in \mathfrak{a}$. $\square$

Capítulo 2

Reticulados em Corpos de Números

A proposta deste Capítulo é uma continuação natural do capítulo anterior, visando apresentar a Teoria Algébrica dos Números necessária à plena compreensão das aplicações a serem desenvolvidas no próximo capítulo.

Tendo em vista a complexidade que se encontra quando se trata do caso geral, restringiremos a família dos corpos a serem considerados.

Iniciamos o estudo de corpos de grau 2. Neste caso caracterizamos os corpos quadráticos, seu anel de inteiros algébricos e explicitamos seu discriminante.

Em seguida introduzimos os corpos ciclotômicos, caracterizando os polinômios ciclotômicos, descrevendo uma base integral e o cálculo do discriminante.

Vale ressaltar que apesar dos resultados enunciados no Teorema 2.2 e no Teorema 2.3 serem de domínio público a técnica aqui adotada é original.

Na seção destinada aos corpos abelianos incluímos o Teorema 2.4 e o Teorema 2.5 cujas demonstrações foram omitidas tendo em vista que



os argumentos utilizados nas respectivas demonstrações fogem do espírito deste trabalho, entretanto provamos o Teorema 2.6 que é uma consequência imediata destes.

Em seguida introduzimos as definições de reticulado, empacotamento esférico, densidade de empacotamento e densidade de centro.

Finalizando, definimos o homomorfismo canônico que é um método algébrico para obtenção de reticulados e descrevemos um reticulado de $\mathbb{R}^n$ que é obtido pela representação geométrica de um ideal $\mathfrak{I}$ do anel dos inteiros algébricos de um corpo de números K de grau n , cuja densidade de centro depende do discriminante de K , da norma de $\mathfrak{I}$ e do menor valor assumido pela função traço, sujeito à certas restrições.

2.1 Corpos Quadráticos

Nesta Seção introduzimos os corpos quadráticos juntamente com a teoria necessária para caracterizar seu anel de inteiros algébricos, base integral e discriminante.

Sejam $K = \mathbb{Q}(\theta)$ um corpo quadrático, ou seja, um corpo de números de grau 2, e

$$f(X) = X^2 + aX + b = \text{irr}(\theta, \mathbb{Z}).$$

Podemos supor

$$\theta = \frac{-a + \sqrt{a^2 - 4b}}{2}.$$

Assim

$$2\theta + a = \sqrt{a^2 - 4b},$$

logo $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{a^2 - 4b})$. Por outro lado, $a^2 - 4b$ é um inteiro que podemos escrever como $a^2 - 4b = r^2d$, sendo d um inteiro livre de quadrados. Finalmente, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{d})$ e deste modo provamos o seguinte resultado:

Proposição 2.1 [6] *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, sendo d um inteiro livre de quadrados.*

A determinação do anel dos inteiros algébricos de $\mathbb{Q}(\sqrt{d})$, com d um inteiro livre de quadrados, depende exclusivamente das propriedades de congruência de d módulo 4. O Teorema seguinte apresenta esta caracterização.

Teorema 2.1 [6] *Sejam d um inteiro livre de quadrados e $K = \mathbb{Q}(\sqrt{d})$. Então $\mathcal{O}_K = \mathbb{Z}[w]$, com*

$$w = \begin{cases} \sqrt{d} & \text{se } d \equiv 2, 3 \pmod{4} \\ \frac{1+\sqrt{d}}{2} & \text{se } d \equiv 1 \pmod{4}. \end{cases}$$

Demonstração. É óbvio que $\mathbb{Z}[w] \subset \mathcal{O}_K$ pois, sendo $w = \sqrt{d}$, w é raiz do polinômio irredutível $X^2 - d \in \mathbb{Z}[X]$ e quando $w = \frac{1+\sqrt{d}}{2}$, w é raiz do polinômio irredutível $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$.

Reciprocamente, seja $\alpha = r + s\sqrt{d} \in \mathcal{O}_K$; $r, s \in \mathbb{Q}$. Se $s = 0$ então $r \in \mathbb{Z}$ e portanto $\alpha \in \mathbb{Z} \subset \mathbb{Z}[w]$. Podemos supor $s \neq 0$, assim

$$\text{irr}(\alpha, \mathbb{Q}) = X^2 - 2rX + (r^2 - ds^2),$$

logo $2r, r^2 - ds^2 \in \mathbb{Z}$ e, consequentemente, $(2r)^2 - d(2s)^2 \in \mathbb{Z}$. Visto que $2r \in \mathbb{Z}$ então $d(2s)^2 \in \mathbb{Z}$ e mostremos que $2s \in \mathbb{Z}$. Suponhamos que $2s \notin \mathbb{Z}$, ou seja, $2s = \frac{x}{y}$, com $(x, y) = 1$. Sendo $y \neq 1$ existe um primo p tal que p^2 divide y^2 . Mas, para que $d(2s)^2$ seja inteiro é necessário que p^2 divida d , contrariando o fato de d ser livre de quadrados e portanto $2s \in \mathbb{Z}$.

Fazendo $r = \frac{u}{2}$, $s = \frac{v}{2}$; $u, v \in \mathbb{Z}$, temos que $u^2 - dv^2 \in 4\mathbb{Z}$. Sendo $u^2 \equiv 0$ ou $1 \pmod{4}$ se $d \equiv 2$ ou $3 \pmod{4}$ a única possibilidade para $u^2 - dv^2 \in 4\mathbb{Z}$ é $u \equiv v \equiv 0 \pmod{2}$ e, portanto, $\alpha \in \mathbb{Z}[\sqrt{d}]$. Assim temos $\mathcal{O}_K = \mathbb{Z}[w]$ se $d \equiv 2$ ou $3 \pmod{4}$.

Entretanto, se $d \equiv 1 \pmod{4}$, $u^2 \equiv v^2 \equiv 1 \pmod{4}$ também é admissível, ou seja, para que $\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{d}$ seja inteiro algébrico é suficiente que u e v tenham a mesma paridade. Logo $u - v = 2t$ o que nos dá $u = 2t + v$ e $\alpha = t.1 + v\left(\frac{1+\sqrt{d}}{2}\right) \in \mathbb{Z}[w]$ e, conseqüentemente, $\mathcal{O}_K = \mathbb{Z}[w]$ se $d \equiv 1 \pmod{4}$. $\square$

No caso em que $d \equiv 2$ ou $3 \pmod{4}$, $\{1, \sqrt{d}\}$ é uma base integral de $\mathbb{Z}[\sqrt{d}]$ e o discriminante vale $4d$. Se $d \equiv 1 \pmod{4}$, $\{1, \frac{1+\sqrt{d}}{2}\}$ é uma base integral de $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ e o discriminante é d . De fato,

$$\mathfrak{D}_K = \begin{vmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{vmatrix}^2 = (-2\sqrt{d})^2 = 4d$$

e

$$\mathfrak{D}_K = \begin{vmatrix} 1 & \frac{1}{2} + \frac{1}{2}\sqrt{d} \\ 1 & \frac{1}{2} - \frac{1}{2}\sqrt{d} \end{vmatrix}^2 = (-\sqrt{d})^2 = d.$$

Exemplo 2.1 Dado $K = \mathbb{Q}(i)$ então $\mathbb{Z}[\sqrt{-1}]$ é o anel dos inteiros algébricos de K e $\mathfrak{D}_K = -4$. Os monomorfismos de K em $\mathbb{C}$ são σ_1 a inclusão, σ_2 a conjugação complexa, isto é,

$$\sigma_1(r + s\sqrt{-1}) = r + s\sqrt{-1} \text{ e } \sigma_2(r + s\sqrt{-1}) = r - s\sqrt{-1}.$$

Logo

$$N_{K/\mathbb{Q}}(r + s\sqrt{-1}) = r^2 + s^2$$

$$Tr_{K/\mathbb{Q}}(r + s\sqrt{-1}) = 2r.$$

Exemplo 2.2 Dado $K = \mathbb{Q}(\sqrt{-3})$ então $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ é o anel dos inteiros de K e $\mathfrak{D}_K = -3$.

2.2 Corpos Ciclotômicos

Os corpos ciclotômicos desempenham papel fundamental na Teoria Algébrica dos Números. Como veremos a seguir é possível caracterizar o anel dos inteiros algébricos de um corpo ciclotômico e, conseqüentemente, seu discriminante e demais parâmetros.

Dado n um inteiro positivo, definimos ξ_n como sendo $e^{\frac{2\pi i}{n}}$, denominamos $\mathbb{Q}(\xi_n)$ o n -ésimo Corpo Ciclotômico e $\phi_n(X) = \prod_{\substack{i=1 \\ (i,n)=1}}^n (X - \xi_n^i)$ o n -ésimo Polinômio Ciclotômico.

2.2.1 Polinômios Ciclotômicos

Com o objetivo de obter informações de $\mathbb{Q}(\xi_n)$, desenvolvemos nesta Seção resultados explorando propriedades de $\phi_n(X)$.

Lema 2.1 [4] *Seja n um inteiro positivo. Então*

$$X^n - 1 = \prod_{d|n} \phi_d(X).$$

Demonstração. Sejam $1 = d_1 < d_2 < \dots < d_s = n$ todos os divisores de n . Então

$$X^n - 1 = \prod_{\substack{i=0 \\ (i,n)=d_1=1}}^{n-1} (X - \xi_n^i) \cdot \prod_{\substack{i=0 \\ (i,n)=d_2}}^{n-1} (X - \xi_n^i) \cdots \prod_{\substack{i=0 \\ (i,n)=d_s}}^{n-1} (X - \xi_n^i),$$

e

$$\prod_{\substack{i=0 \\ (i,n)=d_1}}^{n-1} (X - \xi_n^i) = \phi_{\frac{n}{d_1}}(X) = \phi_n(X), \text{ pois } d_1 = 1.$$

Observe que se $d = (j, n)$ então $\xi_n^j = \xi_{n/d}^{j/d}$. Logo

$$\prod_{\substack{i=0 \\ (i,n)=d}}^{n-1} (X - \xi_n^i) = \prod_{\substack{j=0 \\ (j,t)=1}}^{t-1} (X - \xi_{t/d}^{j/d}) = \prod_{\substack{j=0 \\ (j,t)=1}}^{t-1} (X - \xi_t^j) = \phi_t(X),$$

com $t = \frac{n}{d}$ e $j = \frac{i}{d}$. Repetindo o mesmo argumento em todos os fatores, obtemos

$$X^n - 1 = \phi_{\frac{n}{d_1}}(X) \phi_{\frac{n}{d_2}}(X) \cdots \phi_{\frac{n}{d_s}}(X),$$

como $\frac{n}{d_1}, \dots, \frac{n}{d_s}$ também são todos os divisores de n e, portanto, a demonstração está concluída. $\square$

Lema 2.2 [4] *Seja n um inteiro positivo. Então o n -ésimo polinômio ciclotômico $\phi_n(X)$ tem coeficientes inteiros, ou seja, $\phi_n(X) \in \mathbb{Z}[X]$.*

Demonstração. A demonstração é feita por indução sobre n . No caso em que $n = 1$, temos $\phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Suponhamos que vale para $2, 3, \dots, n-1$ e provemos que vale para n . Sendo

$$X^n - 1 = \prod_{d|n} \phi_d(X) = \phi_n(X) \prod_{\substack{d|n \\ d < n}} \phi_d(X).$$

e fazendo

$$\prod_{\substack{d|n \\ d < n}} \phi_d(X) = f(X) \text{ temos } X^n - 1 = \phi_n(X) \cdot f(X),$$

com $f(X) \in \mathbb{Z}[X]$ por hipótese de indução.

Sejam

$$\phi_n(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0,$$

$$f(X) = X^r + b_{r-1}X^{r-1} + \cdots + b_0;$$

$b_j \in \mathbb{Z}; j = 1, \dots, r-1$. Queremos mostrar que $a_i \in \mathbb{Z}; i = 1, \dots, m-1$.

Suponhamos que $a_{m-1}, a_{m-2}, \dots, a_u \in \mathbb{Z}$ e $a_{u-1} \notin \mathbb{Z}$. Então

$$X^n - 1 = X^{m+r} + (b_{r-1} + a_{m-1})X^{m+r-1} + \cdots + a_0b_0$$



e, concluímos, pela igualdade de polinômios que cada coeficiente de $\phi_n(X).f(X)$ é inteiro, logo $a_{u-1} \in \mathbb{Z}$ o que é absurdo, pois por hipótese $a_{u-1} \notin \mathbb{Z}$. Portanto $\phi_n(X) \in \mathbb{Z}[X]$. $\square$

Lema 2.3 [4] *Seja n um inteiro positivo. Então o n -ésimo polinômio ciclotômico $\phi_n(X)$ é irredutível sobre $\mathbb{Q}$.*

Demonstração. Seja $f(X) = \text{irr}(\xi_n, \mathbb{Q})$ então existe $g(X) \in \mathbb{Z}[X]$, mônico, tal que

$$\phi_n(X) = f(X).g(X)$$

e queremos provar que $f(X) = \phi_n(X)$.

Sejam $K = \mathbb{Q}(\xi_n)$, $\mathcal{O}_K$ o anel dos inteiros algébricos de K , $\mathfrak{p}$ um ideal primo de $\mathcal{O}_K$ e $p \in \mathfrak{p}$ um número primo, $(p, n) = 1$. Se ξ_n^p não é raiz de $f(X)$ então ξ_n^p é raiz de $g(X)$. Tomando $g(X) = b_0 + b_1X + \cdots + b_tX^t$ tem-se que em $\frac{\mathcal{O}_K}{\mathfrak{p}}$,

$$\overline{g(\xi_n^p)} = \overline{b_0 + b_1\xi_n^p + \cdots + b_t(\xi_n^p)^t} = \overline{0}.$$

Consideremos o homomorfismo

$$\begin{aligned} \theta : \frac{\mathcal{O}_K}{\mathfrak{p}} &\rightarrow \frac{\mathcal{O}_K}{\mathfrak{p}} \\ x &\rightarrow x^p \end{aligned}$$

e visto que $p \in \mathfrak{p}$ tem-se que θ é injetiva e, consequentemente, sobrejetiva pois $\frac{\mathcal{O}_K}{\mathfrak{p}}$ é finito. Assim

$$\begin{aligned} \overline{g(\xi_n^p)} &= \overline{b_0 + (b_1\xi_n)^p + \cdots + (b_t\xi_n^t)^p} \\ &= \overline{(b_0 + b_1\xi_n + \cdots + b_t\xi_n^t)^p} = \overline{0} \end{aligned}$$

e, portanto,

$$\overline{g(X)} = \overline{(b_0 + b_1X + \cdots + b_tX^t)^p}.$$

Sabemos que

$$X^n - 1 = \phi_n(X) \cdot \prod_{\substack{d|n \\ d < n}} \phi_d(X) = f(X) \cdot g(X) \cdot \prod_{\substack{d|n \\ d < n}} \phi_d(X)$$

por outro lado, em $\frac{\mathcal{O}_K}{\mathfrak{p}}$,

$$\overline{X^n - 1} = \overline{f(X) \cdot g(X) \cdot \prod_{\substack{d|n \\ d < n}} \phi_d(X)} \quad (2.1)$$

logo $\overline{X^n - 1}$ tem raízes múltiplas, a menos que $g(X)$ seja constante. Derivando o primeiro membro de 2.1, obtemos $\overline{nX^{n-1}}$ que tem $\bar{0}$ como única raiz, pois p não divide n . Como $\bar{0}$ não é raiz de $\overline{X^n - 1}$, então $\overline{X^n - 1}$ não tem raiz múltipla. Com isso concluímos que $g(X)$ é constante e, portanto, $f(X) = \phi_n(X)$. $\square$

Em decorrência dos resultados acima descritos, deduzimos que o n -ésimo polinômio ciclotômico é o polinômio irredutível de ξ_n sobre $\mathbb{Q}$. Denotando por $\phi(n)$ o grau de $\phi_n(X)$, obteremos nos próximos resultados informações úteis sobre a função $\phi(n)$.

Lema 2.4 [4] *Seja n um número inteiro positivo e $\prod_{i=1}^s p_i^{a_i}$ sua fatoração em potências de primos. Então $\phi(n) = \prod_{i=1}^s (p_i - 1)p_i^{a_i-1}$.*

Demonstração. Faremos a demonstração em duas etapas :

1ª Etapa. $\phi(p^a) = (p - 1)p^{a-1}$; se p é um número primo.

2ª Etapa. Se $u, v \in \mathbb{N}^*$, $(u, v) = 1$ então $\phi(uv) = \phi(u)\phi(v)$.

Sabendo que $\phi(n) = \#\{i = 1, \dots, n; (i, n) = 1\}$ então quando $n = p^a$, p primo e $a \geq 1$, temos que

$$\#\{i = 1, \dots, p^a; (i, p^a) = 1\} = p^a - \#\{i = 1, \dots, p^a; (i, p^a) > 1\}.$$

Mas

$$\{i = 1, \dots, p^a; (i, p^a) > 1\} = \{p, 2p, \dots, p^{a-1}p\}$$

cuja cardinalidade é p^{a-1} , ou seja,

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1).$$

Provemos agora a 2ª etapa. Dados $u, v \in \mathbb{Z}$, $(u, v) = 1$, sejam

$$U = \{i = 1, \dots, u; (i, u) = 1\} \text{ e } V = \{i = 1, \dots, v; (i, v) = 1\},$$

com $\#U = \phi(u)$, $\#V = \phi(v)$ e $\#U \times V = \phi(u)\phi(v)$.

Seja

$$\begin{aligned} \gamma_1 : U \times V &\rightarrow \left(\frac{\mathbb{Z}}{u.v.\mathbb{Z}}\right)^* \\ (x, y) &\rightarrow \overline{x.v + y.u} \end{aligned}$$

Quando $(x.v + y.u, u.v) = d \geq 1$ então existe um primo p tal que p divide d , ou seja, p divide $u.v$ e p divide $x.v + y.u$. Sem perda de generalidade suponhamos que p divide u . Visto que p também divide $x.v + y.u$ então p divide $x.v$ o que implica p divide x ou p divide v . Mas $(u, v) = 1$ então p divide x . Por outro lado $x \in U$ então p não divide x , absurdo. Logo $(x.v + y.u, u.v) = 1$ e portanto a função γ_1 está bem definida. A aplicação γ_1 é injetiva pois,

$$\begin{aligned} \gamma_1.(x_1, y_1) &= \gamma_2.(x_2, y_2) \Leftrightarrow \overline{x_1.v + y_1.u} = \overline{x_2.v + y_2.u} \\ &\Leftrightarrow \overline{x_1.v + y_1.u - x_2.v - y_2.u} = \overline{0} \\ &\Rightarrow (x_1.v + y_1.u) - (x_2.v + y_2.u) \in u.v.\mathbb{Z}. \end{aligned}$$

Daí, $v.(x_1 - x_2) + u.(y_1 - y_2) = u.v.t$ logo $v.(x_1 - x_2) = u.t_1$ o que implica u divide $x_1 - x_2$ e, portanto $x_1 = x_2$. Analogamente $y_1 = y_2$. Visto que $(u, v) = 1$ então existem $r \in V$ e $s \in U$ tais que

$$u.r \equiv 1(\text{mod } v) \text{ e } v.s \equiv 1(\text{mod } u).$$

Assim, dados $m \in \mathbb{Z}$; $(m, u.v) = 1$, $x \in U$ e $y \in V$ tais que $m.r \equiv x(\text{mod } u)$ e $m.s \equiv y(\text{mod } v)$ então

$$m \equiv x.v(\text{mod } u) \text{ e } m \equiv y.u(\text{mod } v). (*)$$

Afirmção. $m \equiv x.v + y.u(\text{mod } u.v)$. De fato isto vale se $u.v$ divide $m - (x.v + y.u)$, ou seja, u divide $m - (x.v + y.u)$ e v divide $m - (x.v + y.u)$, ou equivalentemente, u divide $m - x.v$ e v divide $m - y.u$. O que pode ser visto em (*), logo γ_1 é sobrejetiva e, portanto, bijetiva. Assim sendo, $\#U \times V = \#(\frac{\mathbb{Z}}{uv\mathbb{Z}})^*$. Portanto $\phi(uv) = \phi(u)\phi(v)$. $\square$

2.2.2 Base Integral e Discriminante

Destacamos nesta Seção o anel dos inteiros algébricos de um corpo ciclotômico e seu discriminante.

De início consideramos p um número primo ímpar e ignoramos $p = 2$, pois neste caso $\mathbb{Q}(\xi_2) = \mathbb{Q}$. Em seguida exibimos o anel dos inteiros algébricos de um corpo ciclotômico e seu discriminante.

Lema 2.5 [6] *Seja p um número primo ímpar. Então o anel dos inteiros algébricos de $K = \mathbb{Q}(\xi_p)$ é $\mathbb{Z}[\xi_p]$.*

Demonstração. Seja $\alpha \in \mathcal{O}_K$, então existem $a_0, \dots, a_{p-2} \in \mathbb{Q}$ tal que $\alpha = \sum_{i=0}^{p-2} a_i \xi_p^i$. Considere o elemento $\alpha \xi_p^{-k} - \alpha \xi_p \in \mathcal{O}_K$, com $k = 0, \dots, p-2$

e

$$Tr_{K|\mathbb{Q}}(\alpha \xi_p^{-k} - \alpha \xi_p) = Tr_{K|\mathbb{Q}}\left(\sum_{i=0}^{p-2} a_i \xi_p^{i-k} - \sum_{i=0}^{p-2} a_i \xi_p^{i+1}\right) = pa_k.$$

Sejam $b_k = pa_k$, com $k = 0, \dots, p-2$ e $\lambda = 1 - \xi_p$. Então

$$\begin{aligned} p\alpha &= pa_0 + pa_1 \xi_p + \dots + pa_{p-2} \xi_p^{p-2} \\ &= b_0 + b_1 \xi_p + \dots + b_{p-2} \xi_p^{p-2} \\ &= c_0 + c_1 \lambda + \dots + c_{p-2} \lambda^{p-2} \end{aligned} \quad (2.2)$$

com

$$c_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} b_j \in \mathbb{Z} \text{ e } b_i = \sum_{j=i}^{p-2} (-1)^i \binom{j}{i} c_j.$$

Sendo $p = \prod_{i=1}^{p-1} (1 - \xi_p^i) \in \lambda \mathcal{O}_K \cap \mathbb{Z}$, então $p\mathbb{Z} \subset \lambda \mathcal{O}_K \cap \mathbb{Z}$. Visto que $p\mathbb{Z}$ é um ideal maximal, temos

$$\lambda \mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z} \text{ ou } \lambda \mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}.$$

Se $\lambda \mathcal{O}_K \cap \mathbb{Z} = \mathbb{Z}$ então $1 \in \lambda \mathcal{O}_K$, isto é, $1 = \lambda r$, para algum $r \in \mathcal{O}_K$. Aplicando Norma $1 = N(1) = N(\lambda).N(r) = ps$, $s \in \mathbb{Z}$ que é absurdo, pois p é primo. Logo $1 \notin \lambda \mathcal{O}_K$ e, portanto, $\lambda \mathcal{O}_K \cap \mathbb{Z} = p\mathbb{Z}$.

Vamos provar que cada $c_i \in p\mathbb{Z}$ por indução sobre i . Sabemos que $p, p\alpha, c_i \lambda^i$ são elementos de $\lambda \mathcal{O}_K$, $i \geq 1$ e pela Equação 2.2, temos $c_0 \in p\mathbb{Z}$.

Suponha $c_l \in p\mathbb{Z}$, com $1 \leq l \leq k-1$. Então segue

$$p(\alpha - \varepsilon) = \lambda^k (c_k + c_{k+1} \lambda + \dots + c_{p-2} \lambda^{p-k-3}),$$

com

$$\varepsilon = \frac{c_0 + c_1 \lambda + \dots + c_{k-1} \lambda^{k-1}}{p} \in \mathbb{Z}[\lambda].$$

Visto que $p = \prod_{i=1}^{p-1} (1 - \xi_p^i)$ e $1 - \xi_p^i = \lambda \varepsilon_i$, $\varepsilon_i \in \mathbb{Z}[\xi_p]$ então $p = \lambda^{p-1} t$, com $t = \prod_{i=1}^{p-1} \varepsilon_i \in \mathbb{Z}[\xi_p]$. Assim,

$$\lambda^{p-k-1} t (\alpha - \varepsilon) = c_k + c_{k+1} \lambda + \cdots + c_{p-2} \lambda^{p-k-3},$$

com $p - k - 1 > 0$, logo $c_k \in p\mathbb{Z}$ e, portanto, $\mathcal{O}_K = \mathbb{Z}[\xi_p]$. $\square$

O Teorema abaixo enunciado encontra-se em várias referências e cujas demonstrações envolvem um grau de complexidade muito superior àqueles utilizados neste trabalho.

Para nossa conveniência incluímos aqui uma demonstração do mesmo resultado usando apenas argumentos aritméticos.

Teorema 2.2 [8] *Seja n um inteiro positivo. Então o anel dos inteiros algébricos de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$.*

Demonstração. A demonstração é feita por indução sobre o número de divisores primos de n . Sejam $n = p^a \cdot g$, $p \nmid g$, $K = \mathbb{Q}(\xi_g)$, $L = \mathbb{Q}(\xi_n)$, $\lambda = 1 - \xi_{p^a}$ e $m = \phi(p^a)$. Dado

$$\alpha = a_0 + a_1 \xi_{p^a} + \cdots + a_{m-1} \xi_{p^a}^{m-1} \in \mathcal{O}_L,$$

então $\sigma(\alpha) \in \mathcal{O}_L$ para qualquer $\sigma \in \text{Aut}_K^L = \text{Gal}(L/K)$.

Visto que $\sigma_i(\xi_{p^a}) = \xi_{p^a}^i$; $(i, p^a) = 1$ são todos os monomorfismos de $K(\xi_{p^a})$ em $\mathbb{C}$ e α é um inteiro algébrico então

$$\sigma_i(\alpha) = a_0 + a_1 \xi_{p^a}^i + \cdots + a_{m-1} \xi_{p^a}^{i(m-1)}$$

é também um inteiro algébrico e claramente um dos σ'_i 's é a identidade. Então, seja,

$$\begin{aligned}\alpha_1 &= \sigma_1(\alpha) = a_0 + a_1 \xi_{p^a} + \cdots + a_{m-1} \xi_{p^a}^{(m-1)} \\ &\vdots \\ \alpha_m &= \sigma_k(\alpha) = a_0 + a_1 \xi_{p^a}^k + \cdots + a_{m-1} \xi_{p^a}^{k(m-1)}\end{aligned}$$

Colocando o sistema acima na forma matricial, temos

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = \begin{pmatrix} 1 & \xi_{p^a} & \cdots & \xi_{p^a}^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \xi_{p^a}^k & \cdots & \xi_{p^a}^{k(m-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \end{pmatrix}.$$

Sejam $M = (\xi^{ij})$, $i = 1, \dots, n$, $j = 0, \dots, m-1$, $(i, n) = 1$ e M_{i+1} a matriz obtida de M substituindo a i -ésima coluna por

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}.$$

Pela Regra de Cramer $a_i = \frac{\det M_{i+1}}{\det M}$ e do fato de ξ_{p^a} e α_i 's serem inteiros algébricos, deduz-se que $\det M$ é um inteiro algébrico, logo $\det M_{i+1}$ também é um inteiro algébrico. Por outro lado, sabemos que $\det M = p^r$, para algum r . Assim $p^r a_i = \det M_{i+1} \in \mathcal{O}_K \cap \mathbb{Q}(\xi_g)$, logo

$$p^r a_i = \sum_{j=0}^{\phi(g)-1} b_{ij} \xi_g^j$$

e, portanto,

$$p^r \alpha = \sum_{i=0}^{m-1} c_i \xi_{p^a}^i, \quad (2.3)$$

com $c_i \in \mathbb{Z}[\xi_g]$ e queremos mostrar que $r = 0$.

Considere que p não divide c_i , ou seja, $c_i \notin p\mathbb{Z}[\xi_g]$ para algum i . Analisemos dois casos: Caso 1. Quando $n = p^a$. Neste caso cada a_i é um quociente de números inteiros com uma potência de p no denominador. Supondo $r > 0$ e reescrevendo a Equação 2.3, obtemos

$$p^r \alpha = d_0 + d_1 \lambda + \dots + d_{m-1} \lambda^{m-1}; d_i \in \mathbb{Z} \quad (2.4)$$

Mas

$$\prod_{\substack{i=1 \\ (i, p^a)=1}}^{p^a} (X - \xi_{p^a}^i) = \text{irr}(\xi_{p^a}, \mathbb{Q}) = \frac{X^{p^a} - 1}{X^{p^{a-1}} - 1} = \text{irr}(\xi_{p^a}, \mathbb{Q}(\xi_g))$$

então substituindo X por 1, temos $\prod_{\substack{i=1 \\ (i, p^a)=1}}^{p^a} (1 - \xi_{p^a}^i) = p$, por outro lado,

$$N_{K(\xi_{p^a})/K}(1 - \xi_{p^a}^i) = \prod_{\substack{i=1 \\ (i, p^a)=1}}^{p^a} (1 - \xi_{p^a}^i)$$

então

$$N_{K(\xi_{p^a})/K}(1 - \xi_{p^a}^i) = p.$$

Visto que para qualquer grupo finito se fixo um elemento do grupo e multiplico por todos os outros, obtenho o mesmo grupo só que ordenado de maneira diferente. Logo, fixando j , $jt = i$ temos

$$\frac{1 - \xi_{p^a}^i}{1 - \xi_{p^a}^j} = \frac{1 - \xi_{p^a}^{jt}}{1 - \xi_{p^a}^j} = \frac{(1 - \xi_{p^a}^j)(1 + \xi_{p^a}^j + \dots + \xi_{p^a}^{j(t-1)})}{1 - \xi_{p^a}^j} = \sum_{k=0}^{t-1} \xi_{p^a}^{jk}.$$

Analogamente,

$$\frac{1 - \xi_{p^a}^i}{1 - \xi_{p^a}^j} = \frac{1 - \xi_{p^a}^{it}}{1 - \xi_{p^a}^j} = \sum_{k=0}^{t-1} \xi_{p^a}^{ik}.$$

Portanto

$$(1 - \xi_{p^a}^i) = (1 - \xi_{p^a}^j) \cdot \varepsilon_{ij},$$



com $\varepsilon_{ij} \in \mathbb{Z}[\xi_{p^a}]^*$. Assim,

$$p = (1 - \xi_{p^a}) \cdot \varsigma = \lambda^m \cdot \varsigma,$$

com $\varsigma \in \mathbb{Z}[\xi_{p^a}]^*$.

Já vimos que $\lambda\mathcal{O}$ é ideal principal e $\lambda\mathcal{O} \cap \mathbb{Z} = p\mathbb{Z}$, $p\mathbb{Z}$ ideal maximal, então pela Equação 2.4, $d_0 \in \lambda\mathcal{O} \cap \mathbb{Z} = p\mathbb{Z}$ implicando que p divide d_0 e daí, $d_0 = \lambda^m \cdot \varsigma \cdot e_0$. Assim,

$$\frac{\lambda^{m-r} \cdot \varsigma \cdot \alpha}{\lambda} = \frac{\lambda^m \cdot \varsigma \cdot e_0 + d_1 \lambda + \cdots + d_{m-1} \lambda^{m-1}}{\lambda}$$

o que nos dá,

$$\lambda^{m-r-1} \cdot \varsigma^r \cdot \alpha = \lambda^{m-1} \cdot \varsigma \cdot e_0 + d_1 + d_2 \lambda + \cdots + d_{m-1} \lambda^{m-2}.$$

Portanto $d_1 \in \lambda\mathcal{O} \cap \mathbb{Z} = p\mathbb{Z}$ implicando que p divide d_1 . Repetindo essa argumentação temos que p divide $d_0, \dots, d_{m-1}$ o que é absurdo, pois r é mínimo. Portanto $\alpha \in \mathbb{Z}[\xi_{p^a}]$.

Caso 2. Suponhamos que m tenha mais do que dois divisores primos, com $m = [\mathbb{Q}(\xi_n) : K]$, $\mathbb{Q}(\xi_n) = K(\xi_{q^b})$ e $K = \mathbb{Q}(\xi_{p^a \cdot g})$, $n = p^a \cdot q^b \cdot g$; p não divide g , q não divide g . Por hipótese de indução, suponhamos que o anel dos inteiros algébricos de K é $\mathbb{Z}[\xi_{p^a \cdot g}]$. Dado $\alpha \in \mathcal{O}_K \subset \mathbb{Q}(\xi_n)$,

$$\alpha = b_0 + b_1 \xi_n + \cdots + b_{\phi(n)-1} \xi_n^{\phi(n)-1},$$

com $b_i \in \mathbb{Q}$ e queremos mostrar que os b_i 's $\in \mathbb{Z}$. Sabemos que $\xi_n = \xi_{q^b}^i \cdot \xi_{\frac{n}{q^b}}^j$. Assim,

$$\alpha = a_0 + a_1 \xi_{q^b} + \cdots + a_{\phi(q^b)-1} \xi_{q^b}^{\phi(q^b)-1},$$

com $a_i \in \mathbb{Q}(\xi_{\frac{n}{q^b}})$. Logo existe $r \in \mathbb{N}$ tal que $q^r \cdot a_i \in \mathbb{Z}[\xi_{\frac{n}{q^b}}]$, e precisamos mostrar que os $a_i \in \mathbb{Z}[\xi_{\frac{n}{q^b}}]$. Por outro lado, existem $r, s \in \mathbb{Z}$ tais que

$p^r \cdot \alpha \in \mathbb{Z}[\xi_n]$ e $q^s \cdot \alpha \in \mathbb{Z}[\xi_n]$. Por Bézout, existem $u, v \in \mathbb{Z}$ tal que $u \cdot p^r \cdot \alpha + v \cdot q^s \cdot \alpha = 1$. Como $p^r \cdot \alpha \in \mathbb{Z}[\xi_n]$ e $q^s \cdot \alpha \in \mathbb{Z}[\xi_n]$ então

$$u \cdot p^r \cdot \alpha + v \cdot q^s \cdot \alpha = (u \cdot p^r + v \cdot q^s) \alpha = \alpha \in \mathbb{Z}[\xi_n].$$

Portanto o anel dos inteiros algébricos de $\mathbb{Q}(\xi_n)$ é $\mathbb{Z}[\xi_n]$. □

Teorema 2.3 [8] *O discriminante do corpo $K = \mathbb{Q}(\xi_n)$ vale*

$$\mathfrak{D}_K = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Demonstração. Pelo Lema 2.1,

$$X^n - 1 = \prod_{d|n} \phi_d(X) \quad (2.5)$$

derivando os dois membros de 2.5, obtemos

$$nX^{n-1} = \phi'_{d_1}(X) \left(\frac{X^n - 1}{\phi_{d_1}(X)} \right) + \cdots + \phi'_{d_s}(X) \left(\frac{X^n - 1}{\phi_{d_s}(X)} \right);$$

em que $d_1, \dots, d_s$ são os divisores de n .

Substituindo X por ξ_n , calculando a norma e usando a Proposição 1.5, temos

$$n^{\phi(n)} = \pm \mathfrak{D}_K \cdot N_{K/\mathbb{Q}} \left(\prod_{\substack{d|n \\ d < n}} \phi_d(\xi_n) \right).$$

Assim,

$$\mathfrak{D}_K = \pm \frac{n^{\phi(n)}}{N_{K/\mathbb{Q}} \left(\prod_{\substack{d|n \\ d < n}} \phi_d(\xi_n) \right)}.$$

Portanto, resta provar que $N_{K/\mathbb{Q}} \left(\prod_{\substack{d|n \\ d < n}} \phi_d(\xi_n) \right) = \prod_{p|n} p^{\frac{\phi(n)}{p-1}}$. Fazendo,

$$\frac{X^n - 1}{\phi_n(X)} = \frac{\prod_{i=0}^{n-1} (X - \xi_n^i)}{\phi_n(X)}$$

obtemos

$$\prod_{\substack{d|n \\ d < n}} \phi_d(X) = \prod_{\substack{i=1 \\ (i,n) > 1}}^n (X - \xi_n^i)$$

e, consequentemente,

$$\prod_{\substack{d|n \\ d < n}} \phi_d(\xi_n) = \prod_{\substack{i=1 \\ (i,n) > 1}}^n (\xi_n - \xi_n^i) = \prod_{\substack{i=1 \\ (i,n) > 1}}^n (1 - \xi_n^{i-1}).$$

Logo,

$$\begin{aligned} N_{K/\mathbb{Q}} \left(\prod_{\substack{d|n \\ d < n}} \phi_d(\xi_n) \right) &= \prod_{\substack{i=1 \\ (i,n) > 1}}^n N_{K/\mathbb{Q}}(1 - \xi_n^{i-1}) = \prod_{\substack{i=2 \\ (i,n) > 1}}^{n-1} N_{K/\mathbb{Q}}(1 - \xi_n^{i-1}) = \\ &= \prod_{j=1}^s \left[\prod_{\substack{i=2 \\ (i,n) > 1, (\frac{n}{i-1}, n) = p_j^{b_j}}}^{n-1} N_{K/\mathbb{Q}}(1 - \xi_n^{i-1}) \right]. \end{aligned}$$

Quando $n = p^r$ já vimos que $N_{K/\mathbb{Q}}(1 - \xi_{p^r}^i) = p$, e além disso, temos

$$\begin{aligned} N_{K/\mathbb{Q}}(1 - \xi_{p^r}^i) &= N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(N_{K/\mathbb{Q}(\xi_{p^r})}(1 - \xi_{p^r}^i)) \\ &= N_{\mathbb{Q}(\xi_{p^r})/\mathbb{Q}}(1 - \xi_{p^r}^i)^{[K : \mathbb{Q}(\xi_{p^r})]} = p^{[K : \mathbb{Q}(\xi_{p^r})]}. \end{aligned}$$

Já no caso em que $n = n_1 n_2$; $(n_1, n_2) = 1$ temos $N_{K/\mathbb{Q}}(1 - \xi_{p^r}^i) = 1$. De fato, seja

$$X^{n-1} + \dots + X + 1 = \prod_{i=1}^{n-1} (X - \xi_n^i).$$

Substituindo X por 1, obtemos

$$\begin{aligned} n &= \prod_{i=1}^{n-1} (1 - \xi_n^i) \\ &= \prod_{i=1}^{n_2-1} (1 - \xi_n^{in_1}) \cdot \prod_{i=1}^{n_1-1} (1 - \xi_n^{in_2}) \cdot \prod_{\substack{k=1 \\ n_1 \nmid k, n_2 \nmid k}}^{n-1} (1 - \xi_n^k) \\ &= \prod_{i=1}^{n_2-1} (1 - \xi_{n_2}^i) \cdot \prod_{i=1}^{n_1-1} (1 - \xi_{n_1}^i) \cdot \prod_{\substack{k=1 \\ n_1 \nmid k, n_2 \nmid k}}^{n-1} (1 - \xi_n^k). \end{aligned}$$

$$\log 1 = \prod_{\substack{k=1 \\ n_1 \nmid k, n_2 \nmid k}}^{n-1} (1 - \xi_n^k) \text{ e, portanto, } 1 = N_{K/\mathbb{Q}} \left(\prod_{\substack{k=1 \\ n_1 \nmid k, n_2 \nmid k}}^{n-1} (1 - \xi_n^k) \right).$$

Diante de tais considerações, segue que

$$N_{K/\mathbb{Q}}(1 - \xi_n^i) = \begin{cases} p^{[K:\mathbb{Q}(\xi_{p^r})]} & \text{se } \frac{n}{(i,n)} = p^r \\ 1 & \text{caso contrário,} \end{cases}$$

mas queremos, $\frac{n}{(i-1,n)} = p_j^{b_j}$; $(i,n) > 1$. Sendo

$$n = p_1^{a_1} \cdots p_s^{a_s} \text{ e } i-1 = p_1^{a_1} \cdots p_s^{a_s-1} \cdot v; \quad v = 1, \dots, p_s^{a_s} - 1,$$

então,

$$i-1 = \frac{n}{p_j^{b_j}} v, \quad v = 1, \dots, p_j^{b_j} - 1$$

e

$$(i-1, n) = \frac{n}{p_j^{b_j}}; \quad b_j \leq a_j.$$

Visto que $v = 1, \dots, p_j^{b_j} - 1$; p_j não divide v , então existe um único $v \in \{1, \dots, p-1\}$ tal que

$$i = \frac{n}{p_j^{b_j}} v + 1 \equiv 0 \pmod{p_j}.$$

Logo $(i-1, n) > p_j$ implicando $b_j = a_j$ e, portanto,

$$\begin{aligned}
& \prod_{j=1}^s \left[\prod_{\substack{i=2 \\ (i,n) > 1, (\frac{n}{i-1}, n) = p_j^{b_j}}}^{n-1} N_{K/\mathbb{Q}}(1 - \xi_n^{i-1}) \right] \\
&= \prod_{j=1}^s \left[\prod_{\substack{i=\frac{n}{p_j}v+1 \\ v=1, \dots, p_j^{a_j}-1, i \equiv 0 \pmod{p_j}}}^{p_j^{a_j}-1} N_{K/\mathbb{Q}}(1 - \xi_n^{\frac{n}{p_j}v+up_j}) \right] \\
&= \prod_{j=1}^s \left[\prod_{\substack{i=\frac{n}{p_j}v+1 \\ v=1, \dots, p_j^{a_j}-1, i \equiv 0 \pmod{p_j}}}^{p_j^{a_j}-1} N_{K/\mathbb{Q}}(1 - \xi_n^{\frac{n}{p_j}v+up_j}) \right] \\
&= \prod_{j=1}^s \left[\prod_{\substack{u=0 \\ v: \text{conveniente}}}^{p_j^{a_j}-1} N_{K/\mathbb{Q}}(1 - \xi_{p_j^{a_j}}^{v+up_j}) \right] \\
&= \prod_{j=1}^s \left[\prod_{u=0}^{p_j^{a_j}-1} N_{\mathbb{Q}(\xi_{p_j^{a_j}})/\mathbb{Q}}(N_{K/\mathbb{Q}(\xi_{p_j^{a_j}})}(1 - \xi_{p_j^{a_j}}^{v+up_j})) \right] \\
&= \prod_{j=1}^s \left[\prod_{u=0}^{p_j^{a_j}-1} N_{\mathbb{Q}(\xi_{p_j^{a_j}})/\mathbb{Q}}(1 - \xi_{p_j^{a_j}}^{v+up_j})^{\phi(n)/\phi(p_j^{a_j})} \right] \\
&= \prod_{j=1}^s \left[p_j^{\phi(n)/\phi(p_j^{a_j})} \right]^{p_j^{a_j}-1} = \prod_{j=1}^s \left[p_j^{\phi(n)/p_j-1} \right].
\end{aligned}$$

Portanto

$$\mathfrak{D}_K = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

□

Exemplo 2.3 *O discriminante de $\mathbb{Q}(\xi_{20})$ é $2^8 \cdot 5^6$, à menos de sinal.*

Exemplo 2.4 *O discriminante de $\mathbb{Q}(\xi_3)$ é ± 3 .*

Observe que já conhecíamos o valor do discriminante de $\mathbb{Q}(\xi_3)$, pois $\mathbb{Q}(\xi_3) = \mathbb{Q}(\sqrt{-3})$.

2.3 Corpos Abelianos

Dizemos que um corpo de números K é abeliano se K é uma extensão galoisiana dos racionais e seu grupo de Galois é abeliano.

Quando um corpo de números K está contido em um corpo ciclotômico segue, da Teoria de Galois, que K é um corpo abeliano. A recíproca desta afirmação também é válida e aqui será destacada como sendo:

Teorema 2.4 [8] (Kronecker - Weber) *Dado um corpo abeliano K então existe um número inteiro n tal que $K \subseteq \mathbb{Q}(\xi_n)$.*

O cálculo do discriminante de um corpo de números é definido, originalmente, sobre uma base integral, cuja obtenção é, geralmente, um problema complexo. Assim sendo, existem vários resultados que permitem obter o valor do discriminante de um corpo de números sem conhecimento de base integral. Dentre tais resultados destaca-se o Teorema de Hasse-Fórmula do Condutor-Discriminante ([8]) cuja consequência é o resultado abaixo.

Teorema 2.5 [5] *Sejam p um número primo ímpar, r um inteiro positivo e $K \subset \mathbb{Q}(\xi_{p^r})$, $[K : \mathbb{Q}] = up^j$; p não divide u . Então $\mathfrak{D}_K = \pm p^v$, sendo*

$$v = u[(j+2)p^j - \frac{p^{j+1} - 1}{p - 1}] - 1.$$

O próximo resultado explicita uma base integral para uma família particular de corpos de números, que no caso em que K é uma extensão de grau 3, ou seja, uma cúbica, será uma ferramenta importante na manipulação dos exemplos do capítulo seguinte.

Teorema 2.6 *Sejam $K \subset \mathbb{Q}(\xi_p)$; p primo, $r = [\mathbb{Q}(\xi_p) : K]$, $s = [K : \mathbb{Q}]$, $\theta = T_{\mathbb{Q}(\xi_p)/K}(\xi_p)$ e $g \in \mathbb{Z}$ tal que σ_g gera $G = \text{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$. Então $K = \mathbb{Q}(\theta)$ e $\mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_{g^s}(\theta)$ é o anel dos inteiros algébricos de K . Além disso,*

$$\mathfrak{D}_K = \pm p^{[K : \mathbb{Q}] - 1}.$$

Demonstração. Inicialmente, devemos mostrar, que $K = \mathbb{Q}(\theta)$. Evidentemente $\mathbb{Q}(\theta) \subset K$, pois $\theta \in K$.

Sendo

$$\text{Gal}(\mathbb{Q}(\xi_p)/K) = \{\sigma_{g^s}, \sigma_{g^{2s}}, \dots, \sigma_{g^{rs}}\} \text{ e } \theta = \xi_p^{g^s} + \cdots + \xi_p^{g^{rs}}$$

então $\sigma_g(\theta), \dots, \sigma_{g^s}(\theta) \in \mathbb{Q}(\theta)$, pois $\mathbb{Q}(\theta)$ é uma extensão galoisiana de $\mathbb{Q}$.

Sejam $a_1, \dots, a_s \in \mathbb{Q}$ tais que

$$a_1\sigma_g(\theta) + \cdots + a_s\sigma_{g^s}(\theta) = 0. \quad (2.6)$$

Visto que $\sigma_{g^i}(\theta) = \xi_p^{g^{s+i}} + \cdots + \xi_p^{g^{rs+i}}$, se $\xi_p^{g^{t_1s+i_1}} = \xi_p^{g^{t_2s+i_2}}$, com $1 \leq t_1, t_2 \leq r$ e $1 \leq i_1, i_2 \leq s$ então $t_1 = t_2$ e $i_1 = i_2$. Com isso, a Equação 2.6, pode ser reescrita como $\sum_{i=1}^{p-1} b_i \xi_p^i = 0$, sendo

$$\{b_i; i = 1, \dots, p-1\} = \{a_i; i = 1, \dots, s\}.$$

Por outro lado, $\{\xi_p^i; i = 1, \dots, p-1\}$ é um conjunto linearmente independente sobre $\mathbb{Q}$, logo $b_i = 0; i = 1, \dots, p-1$ e, consequentemente, $a_i = 0; i = 1, \dots, s$, ou seja $[\mathbb{Q}(\theta) : \mathbb{Q}] \geq s$.

Já que $\mathbb{Q}(\theta) \subset K$ e $[K : \mathbb{Q}] = s$ temos $K = \mathbb{Q}(\theta)$. É claro que

$$\mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_{g^s}(\theta) \subset \mathcal{O}_K$$

pois, $\sigma_{g^i}(\theta) \in \mathbb{Z}[\xi_p] \cap K$. Provaremos agora a recíproca. Seja, pois, $\alpha \in \mathcal{O}_K$ então existem $a_1, \dots, a_s \in \mathbb{Q}$ tais que $\alpha = \sum_{i=1}^s a_i \sigma_{g^i}(\theta)$, visto que $\{\sigma_g(\theta), \dots, \sigma_{g^s}(\theta)\}$ é base de $K/\mathbb{Q}$. Então, como $\alpha \in \mathbb{Z}[\xi_p]$ e repetindo o argumento utilizado na demonstração de $K = \mathbb{Q}(\theta)$, podemos concluir que $a_i \in \mathbb{Z}$, $i = 1, \dots, s$; isto é,

$$\mathcal{O}_K = \mathbb{Z}\sigma_g(\theta) + \cdots + \mathbb{Z}\sigma_{g^s}(\theta).$$

O valor do discriminante de K é obtido via Teorema 2.5. □

2.4 Reticulados

Sejam V um espaço vetorial de dimensão n sobre um corpo K , A um subanel de K e $v_1, \dots, v_r$, $r \leq n$, vetores linearmente independentes de V . Chamamos de A -reticulado com base $(v_1, \dots, v_r)$ ao conjunto dos elementos da forma

$$x = \sum_{i=1}^r a_i v_i,$$

com $a_i \in A$.

Doravante em qualquer citação de reticulado, será suposto que $K = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $r = n$.

Dados um reticulado Λ com base $(v_1, \dots, v_n)$ e $c_1, \dots, c_n$ elementos quaisquer de Λ , sejam $a_{ij} \in \mathbb{Z}$ tais que $c_i = \sum_{j=1}^n a_{ij} v_j$. É fato conhecido que uma condição necessária e suficiente para que $(c_1, \dots, c_n)$ seja base de Λ é que $\det(a_{ij})$ seja um elemento inversível de $\mathbb{Z}$.

Exemplo 2.5 $\Lambda = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1, 0)$ e $e_2 = (0, 1)$.

Exemplo 2.6 $\Lambda = \{(a, b) \in \mathbb{Z}^2; a + b \equiv 0 \pmod{2}\}$ é um reticulado gerado pelos vetores $v_1 = (2, 0)$ e $v_2 = (1, 1)$.

Um *empacotamento esférico* em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que a interseção de duas tenha no máximo um ponto; chamamos simplesmente de empacotamento. Pode-se descrever um empacotamento simplesmente indicando o conjunto dos centros das esferas e o raio. Um *empacotamento reticulado* é um empacotamento em que o conjunto dos centros forma um reticulado Λ de $\mathbb{R}^n$ e, a menos que se diga o contrário, doravante todos os empacotamentos considerados serão reticulados, e quando o conjunto dos centros for Λ , dizemos que o empacotamento é associado a Λ .

Dado um empacotamento em $\mathbb{R}^n$, define-se a sua *densidade de empacotamento* como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

A seguir, introduzimos os elementos básicos que possibilitarão obter uma expressão para a densidade de um empacotamento.

Seja $\Lambda \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$ -base $\beta = \{m_1, \dots, m_n\}$. Então o conjunto

$$\mathcal{R}_\beta = \{x \in \mathbb{R}^n; x = \sum_{i=1}^n \lambda_i m_i, 0 \leq \lambda_i < 1\}$$

é dita a *região fundamental* de Λ , com relação à base β .

O espaço euclidiano $\mathbb{R}^n$ é a união disjunta dos conjuntos

$$C_v = \{x \in \mathbb{R}^n; x = y + v, y \in \mathcal{R}_\beta, v \in \Lambda\};$$

que são translações da região fundamental $\mathcal{R}_\beta$. Consideremos um empacotamento associado a Λ . Para o cálculo da proporção coberta pelas esferas, basta calcular a proporção na região fundamental $\mathcal{R}_\beta$; é o que faremos a seguir.

Fazendo $m_i = (m_{i1}, \dots, m_{in}) \in \mathbb{R}^n, i = 1, \dots, n$, o volume de $\mathcal{R}_\beta, v(\mathcal{R}_\beta)$ é o módulo do determinante da matriz

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nn} \end{pmatrix}.$$

O volume de $\mathcal{R}_\beta$ independe da base β , pois a matriz de mudança de base é inversível com entradas inteiras, ou seja, tem determinante ± 1 , logo faz sentido definir o volume de Λ como sendo o volume de uma região fundamental, e será denotado por $v(\Lambda)$.

Apenas temos interesse pelo empacotamento associado ao reticulado Λ tal que as esferas tenham raio máximo. Para determinação deste raio, observe que fixado $c > 0$, a interseção do conjunto compacto $\{x \in \mathbb{R}^n; |x| \leq c\}$ com o reticulado Λ é um conjunto finito, logo o número $\Lambda_{\min} = \min\{|v|; v \in \Lambda, v \neq 0\}$ está bem definido.

Note que $\rho = \Lambda_{\min}/2$ é o maior raio para o qual é possível distribuir esferas centradas em cada ponto do reticulado Λ e obtermos um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. Com isto, quando citamos densidade do reticulado Λ , ficará implícito que estamos falando da densidade de empacotamento com esferas de raio ρ associado a este reticulado, e que será denotada por $\Delta(\Lambda)$.

Denotando por $B(\rho)$ a esfera com centro na origem e raio ρ , temos



$$\begin{aligned}\Delta(\Lambda) &= \frac{\text{Volume da região fundamental coberta pelas esferas}}{\text{Volume da região fundamental}} \\ &= \frac{v(B(\rho))}{v(\mathcal{R})} = v(B(1)) \cdot \frac{\rho^n}{v(\Lambda)}.\end{aligned}$$

É conveniente o uso de um outro parâmetro, a saber a densidade de centro, cuja expressão é:

$$\delta(\Lambda) = \frac{\rho^n}{v(\Lambda)}.$$

Exemplo 2.7 Seja $\Lambda = \mathbb{Z}^n$ um reticulado de $\mathbb{R}^n$, gerado pelos vetores: $v_1 = (1, 0, \dots, 0)$, $v_2 = (0, 1, \dots, 0), \dots, v_n = (0, 0, \dots, 1)$. A forma quadrática $|v|^2 = x_1^2 + \dots + x_n^2$ assume o mínimo quando um dos $x_i = 1$ para $i = 1, \dots, n$ e os demais nulos, e este valor é 1, logo $\rho = \frac{1}{2}$. Visto que $v(\Lambda) = |\det M|$, e M neste caso é a matriz identidade então $v(\Lambda) = 1$ e, portanto, $\delta(\Lambda) = \frac{1}{2^n}$.

2.5 O Homomorfismo Canônico

Nesta Seção definimos o homomorfismo canônico de um corpo de números K , o qual usamos para descrever reticulados em $\mathbb{R}^n$, originados de submódulos do anel dos inteiros algébricos de K .

Sejam K um corpo de números de grau n e $\sigma_i : K \mapsto \mathbb{C}$, $i = 1, \dots, n$ os monomorfismos de K em $\mathbb{C}$. Se $\sigma_i(K) \subseteq \mathbb{R}$ diz-se que σ_i é *real*, caso contrário σ_i é dito *imaginário*. Quando todos os monomorfismos são reais diz-se que K é um *corpo totalmente real* e quando os monomorfismos são todos imaginários diz-se que K é um *corpo totalmente imaginário*.

Definimos, a seguir, o homomorfismo canônico para o caso geral. Sejam K um corpo de números de grau n , r_1 a quantidade de monomorfismos



reais e $2r_2$ a quantidade de monomorfismos imaginários. Podemos ordenar os monomorfismos $\sigma_1, \dots, \sigma_n$ de tal modo que $\sigma_1, \dots, \sigma_{r_1}$ sejam os monomorfismos reais e $\sigma_{r_1+r_2+i} = \overline{\sigma_{r_1+i}}$; $i = 1, \dots, r_2$ assim, o homomorfismo canônico

$$\sigma_K : K \rightarrow \mathbb{R}^n$$

é definido por:

$$\sigma_K(x) = (\sigma_1(x), \dots, \sigma_{r_1}(x), R\sigma_{r_1+1}(x), I\sigma_{r_1+1}(x), \dots, R\sigma_{r_1+r_2}(x), I\sigma_{r_1+r_2}(x)),$$

com as notações $R(z)$ e $I(z)$ representando as partes real e imaginária do número complexo z , respectivamente.

Teorema 2.7 [7] *Sejam K um corpo de números de grau n , $\sigma_1, \dots, \sigma_n$ os monomorfismos de K em $\mathbb{C}$ e $M \subseteq K$, um $\mathbb{Z}$ -módulo livre de posto n com $\mathbb{Z}$ -base $\{\alpha_1, \dots, \alpha_n\}$. Então $\sigma_K(M)$ é um reticulado em $\mathbb{R}^n$ com volume*

$$v(\sigma_K(M)) = 2^{-r_2} \cdot |\det(\sigma_i(\alpha_j))|.$$

Demonstração. Sendo $\{\alpha_1, \dots, \alpha_n\}$ uma base de M , mostraremos que

$$\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$$

é uma base de $\sigma_K(M)$. No caso em K é totalmente real,

$$\sigma(\alpha_i) = (\sigma_1(\alpha_i), \dots, \sigma_n(\alpha_i)),$$

$i = 1, \dots, n$. Seja

$$D = \begin{pmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{pmatrix}.$$

Aplicando as propriedades de determinante em D , obtemos

$$\det D = \det((\sigma_i(\alpha_j))).$$

Por outro lado, sabemos que

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

logo

$$(\det D)^2 = \Delta[\alpha_1, \dots, \alpha_n]$$

e pelo Teorema 1.5, $\Delta[\alpha_1, \dots, \alpha_n] \neq 0$. Logo $\det D \neq 0$ implicando que $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ são vetores linearmente independentes sobre $\mathbb{R}$.

Por construção $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ geram $\sigma_K(M)$ logo $\{\sigma(\alpha_1), \dots, \sigma(\alpha_n)\}$ é uma base de $\sigma_K(M)$ e, portanto, $\sigma_K(M)$ é um reticulado.

Para o caso em que K é totalmente imaginário, prova-se com argumentos similares que $\sigma_K(M)$ é um reticulado.

Mostremos que $v(\sigma_K(M)) = 2^{-r_2} \cdot |\det(\sigma_i(\alpha_j))|$, quando K é totalmente imaginário. Nesse caso

$$\sigma(\alpha_i) = (R\sigma_1(\alpha_i), I\sigma_1(\alpha_i), \dots, R\sigma_{r_2}(\alpha_i), I\sigma_{r_2}(\alpha_i)).$$

Seja

$$D = \begin{pmatrix} R\sigma_1(\alpha_1) & I\sigma_1(\alpha_1) & \cdots & R\sigma_{r_2}(\alpha_1) & I\sigma_{r_2}(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ R\sigma_1(\alpha_n) & I\sigma_1(\alpha_n) & \cdots & R\sigma_{r_2}(\alpha_n) & I\sigma_{r_2}(\alpha_n) \end{pmatrix}$$

Somando à cada coluna de ordem ímpar multiplicada pela unidade imaginária i a coluna seguinte, obtemos a matriz

$$D_1 = \begin{pmatrix} \sigma_1(\alpha_1) & I\sigma_1(\alpha_1) & \cdots & \sigma_{r_2}(\alpha_1) & I\sigma_{r_2}(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & I\sigma_1(\alpha_n) & \cdots & \sigma_{r_2}(\alpha_n) & I\sigma_{r_2}(\alpha_n) \end{pmatrix}$$

Multiplicando as colunas de ordem par por $-2i$ e a cada uma delas adicionando a coluna anterior, obtemos a matriz

$$D_2 = \begin{pmatrix} \sigma_1(\alpha_1) & \bar{\sigma}_1(\alpha_1) & \cdots & \sigma_{r_2}(\alpha_1) & \bar{\sigma}_{r_2}(\alpha_1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \bar{\sigma}_1(\alpha_n) & \cdots & \sigma_{r_2}(\alpha_n) & \bar{\sigma}_{r_2}(\alpha_n) \end{pmatrix}$$

Em função das operações elementares aqui adotadas temos:

$$\det D_2 = (-2i)^{r_2} \cdot \det D_1 \text{ e } \det D_1 = \det D.$$

Assim $\det D = (-2i)^{-r_2} \cdot \det D_2$. Mas $\bar{\sigma}_i = \sigma_{r_2+i}$ então

$$v(\sigma_K(M)) = |\det D| = 2^{-r_2} \cdot |\det(\sigma_i(\alpha_j))|.$$

□

Exemplo 2.8 *Sejam $K = \mathbb{Q}(\sqrt{6})$ e $M = \mathbb{Z}[\sqrt{6}]$ o anel dos inteiros algébricos de K , com base $\{1, \sqrt{6}\}$. Já que K é totalmente real então $r_2 = 0$, logo,*

$$v(\sigma_K(M)) = \left| \det \begin{pmatrix} 1 & \sqrt{6} \\ 1 & -\sqrt{6} \end{pmatrix} \right| = 2\sqrt{6}.$$

Exemplo 2.9 *Sejam $K = \mathbb{Q}(\sqrt{-7})$ e $M = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ o anel dos inteiros algébricos de K , com base $\left\{1, \frac{1+\sqrt{-7}}{2}\right\}$. Como K é totalmente imaginário então $r_2 = 1$ e, portanto,*

$$v(\sigma_K(M)) = \frac{1}{2} \left| \det \begin{pmatrix} 1 & \frac{1+\sqrt{-7}}{2} \\ 1 & \frac{1-\sqrt{-7}}{2} \end{pmatrix} \right| = \frac{1}{2} \sqrt{7}.$$

Teorema 2.8 [6] *Sejam K um corpo de números de grau n , com discriminante $\mathfrak{D}_K$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_K$. Então o volume de $\sigma_K(\mathfrak{a})$ em $\mathbb{R}^n$, vale*

$$v(\sigma_K(\mathfrak{a})) = 2^{-r_2} \cdot |\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a}).$$

Demonstração. Seja $\{\alpha_1, \dots, \alpha_n\}$ uma base do ideal $\mathfrak{a}$ e visto que $\mathcal{O}_K \subseteq K$, segue pelo Teorema 2.7, $v(\sigma_K(\mathfrak{a})) = |\det D|$, sendo

$$|\det D| = 2^{-r_2} \cdot |\det(\sigma_i(\alpha_j))|.$$

Por outro lado, temos

$$|\Delta[\alpha_1, \dots, \alpha_n]|^{\frac{1}{2}} = |\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})$$

e

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

Logo

$$v(\sigma_K(\mathfrak{a})) = 2^{-r_2} \cdot |\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a}).$$

□

Chamamos de *realização geométrica* de um ideal $\mathfrak{a}$ ao reticulado $\sigma_K(\mathfrak{a})$.

A expressão para a densidade de centro desses reticulados assume a forma

$$\delta(\sigma_K(\mathfrak{a})) = \frac{2^{r_2} \cdot \rho^n}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})}.$$

Lema 2.6 *Sejam K um corpo de números e $x \in K$. Então*

$$|\sigma_K(x)|^2 = c \cdot \text{Tr}_{K/\mathbb{Q}}(x\bar{x}),$$

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

Demonstração. No caso em que K é totalmente real, para $x \in K$, $\sigma_K(x) = (\sigma_1(x), \dots, \sigma_n(x))$. Assim,

$$\begin{aligned} |\sigma_K(x)|^2 &= \sigma_1(x)^2 + \cdots + \sigma_n(x)^2 = \sigma_1(x^2) + \cdots + \sigma_n(x^2) \\ &= \sigma_1(x\bar{x}) + \cdots + \sigma_n(x\bar{x}) = T_{K/\mathbb{Q}}(x\bar{x}). \end{aligned}$$

Dado $x \in K$ e sendo K totalmente imaginário, temos

$$\sigma_K(x) = (R\sigma_1(x), I\sigma_1(x), \dots, R\sigma_{\frac{n}{2}}(x), I\sigma_{\frac{n}{2}}(x)) \text{ e}$$

$$\begin{aligned} |\sigma_K(x)|^2 &= (R\sigma_1(x))^2 + (I\sigma_1(x))^2 + \cdots + (R\sigma_{\frac{n}{2}}(x))^2 + (I\sigma_{\frac{n}{2}}(x))^2 \\ &= \sigma_1(x)\bar{\sigma}_1(x) + \cdots + \sigma_{\frac{n}{2}}(x)\bar{\sigma}_{\frac{n}{2}}(x) \\ &= \sigma_1(x)\sigma_1(\bar{x}) + \cdots + \sigma_{\frac{n}{2}}(x)\sigma_{\frac{n}{2}}(\bar{x}) \\ &= \sigma_1(x\bar{x}) + \cdots + \sigma_{\frac{n}{2}}(x\bar{x}). \end{aligned}$$

Por outro lado,

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \cdots + \sigma_{\frac{n}{2}}(x\bar{x}) + \bar{\sigma}_1(x\bar{x}) + \cdots + \bar{\sigma}_{\frac{n}{2}}(x\bar{x}).$$

Visto que $\bar{\sigma}_1(x\bar{x}) = \sigma_1(x\bar{x})$ então

$$Tr_{K/\mathbb{Q}}(x\bar{x}) = 2(\sigma_1(x\bar{x}) + \cdots + \sigma_{\frac{n}{2}}(x\bar{x})),$$

assim

$$\frac{1}{2}Tr_{K/\mathbb{Q}}(x\bar{x}) = \sigma_1(x\bar{x}) + \cdots + \sigma_{\frac{n}{2}}(x\bar{x}).$$

Portanto $|\sigma_K(x)|^2 = \frac{1}{2} \cdot Tr_{K/\mathbb{Q}}(x\bar{x})$. □

Observação 2.1 Fazendo $t_a = \min\{Tr_{K/\mathbb{Q}}(x\bar{x}); x \neq 0, x \in a\}$ para um corpo de números K , então:

1.

$$\delta(\sigma_K(\mathfrak{a})) = \frac{\left(\frac{\sqrt{t}}{2}\right)^n}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})} = \frac{\left(\sqrt{\frac{t}{4}}\right)^n}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})} = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})}$$

se K é totalmente real e

2.

$$\delta(\sigma_K(\mathfrak{a})) = \frac{2^{\frac{n}{2}} \cdot \left(\frac{\sqrt{\frac{1}{2}t}}{2}\right)^n}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})} = \frac{2^{\frac{n}{2}} \cdot \left(\frac{\sqrt{t}}{2}\right)^n}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})} = \frac{\left(\frac{t}{4}\right)^{\frac{n}{2}}}{|\mathfrak{D}_K|^{\frac{1}{2}} \cdot N(\mathfrak{a})}$$

se K é totalmente imaginário. Portanto a expressão é a mesma para ambos os casos.

Exemplo 2.10 Sejam $K = \mathbb{Q}(i)$ e $\mathbb{Z}[\sqrt{-1}]$ o anel dos inteiros algébricos de K . Dado $x = a + bi \in \mathbb{Z}[\sqrt{-1}]$. Então $x\bar{x} = a^2 + b^2$, $\text{Tr}_{K/\mathbb{Q}}(x\bar{x}) = 2(a^2 + b^2)$ e $t = 2$. Visto que $\mathfrak{D}_K = -4$ e $N(\mathbb{Z}[\sqrt{-1}]) = 1$ temos

$$\delta(\sigma_K(\mathbb{Z}[\sqrt{-1}])) = \frac{1}{4}.$$

Capítulo 3

Cúbicas e Aplicações

Neste Capítulo propomos o desenvolvimento de aplicações dos resultados apresentados nos capítulos anteriores, mais precisamente: calcular a densidade de centro dos reticulados obtidos.

Visto que se trata de um capítulo de aplicações, alguns resultados enunciados serão demonstrados e outros não; entretanto tais demonstrações se encontram na referência que acompanha o resultado.

Nosso maior desafio no cálculo efetivo da densidade de centro é minimizar a forma quadrática, caracterizada na 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.

Quando se trata do corpo $\mathbb{Q}(\xi_p)$ apresentamos três expressões para a forma quadrática e observamos que no ideal principal gerado por $1 - \xi_p$ o menor valor assumido pela forma quadrática é $2.p$. Visto que o discriminante do corpo e a norma do ideal são funções de p , a densidade de centro é uma expressão em p .

Ao estudar os reticulados obtidos de cúbicas, dividimos estas em duas



categorias: cúbicas não galoisianas e cúbicas galoisianas.

Na análise das cúbicas não galoisianas, restringimo-nos àquelas da forma $\mathbb{Q}(\sqrt[3]{d})$, com d um inteiro positivo 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 ou utilizando-se de métodos computacionais. No caso de um ideal do anel dos inteiros algébricos de $\mathbb{Q}(\sqrt[3]{d})$ a forma quadrática é minimizada com valores inteiros e ainda satisfazendo condições que caracterizam os elementos do ideal. Visto que o discriminante de $\mathbb{Q}(\sqrt[3]{d})$ é obtido pela Proposição 1.5 e a norma de um ideal principal é obtido como consequência do Teorema 1.14 calculamos, explicitamente a densidade de centro de alguns reticulados; tendo obtido 0,1065 como a maior densidade de centro.

O Lema de Kummer é de fundamental importância neste contexto e se encontra enunciado sob o Lema 1.7. Com este resultado podemos descrever geradores de ideais primos e obter grau residual e índice de ramificação.

Em se tratando das cúbicas galoisianas sabemos, pelo Teorema de Kronecker-Weber, que estas estão contidas em algum corpo do tipo $\mathbb{Q}(\xi_n)$ e, em vista da complexidade do caso geral, restringimos o nosso estudo às cúbicas contidas em $\mathbb{Q}(\xi_{p^r})$, p : primo e $r \geq 1$.

Esta restrição implica que $p = 3$ e $r > 1$ ou p é um primo congruente a 1, módulo 3.

Visto que, nestes casos $G = \text{Gal}(\mathbb{Q}(\xi_{p^r}), \mathbb{Q})$ é cíclico então a existência e unicidade da cúbica contida em $\mathbb{Q}(\xi_{p^r})$ é assegurada, via Teoria de Galois, pela existência e unicidade do subgrupo de G de índice 3.

Esta mesma unicidade nos assegura que a única cúbica contida em $\mathbb{Q}(\xi_{3^r})$, $r > 1$, é a mesma contida em $\mathbb{Q}(\xi_9)$, isto é, estudar a única cúbica contida



em $\mathbb{Q}(\xi_{3^r})$ equivale a estudar o corpo $\mathbb{Q}(\xi_9 + \xi_9^{-1})$.

Analogamente, quando $p \equiv 1 \pmod{3}$, a única cúbica contida em $\mathbb{Q}(\xi_{p^r})$ é aquela contida em $\mathbb{Q}(\xi_p)$.

Por isso, as cúbicas galoisianas que nos propomos estudar são, em resumo, $\mathbb{Q}(\xi_9 + \xi_9^{-1})$ e a única cúbica contida em $\mathbb{Q}(\xi_p)$, quando p é um primo congruente a 1 módulo 3.

Finalizando, abordamos alguns reticulados de posto 3, não obtidos pelo Método de Minkowski. Para tais casos calculamos a densidade de centro e constatamos que a maior densidade de centro obtida dentre todos os exemplos foi justamente com essa metodologia, que julgamos ser uma generalização daquela desenvolvida por Minkowski.

3.1 Reticulados em Corpos Quadráticos

Esta Seção tem a finalidade de calcular a densidade de centro de reticulados de posto 2 em $\mathbb{R}^2$.

Sabemos que todo corpo quadrático é da forma $K = \mathbb{Q}(\sqrt{d})$, 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 2.1:

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{(\frac{t_{\mathcal{O}_K}}{4})}{|\mathfrak{D}_K|^{\frac{1}{2}}}.$$

Exemplo 3.1 *Sejam $K = \mathbb{Q}(\sqrt{6})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{6}]$ e $\mathfrak{D}_K = 24$. Dado $\alpha = a + b\sqrt{6} \in \mathcal{O}_K$, $\alpha\bar{\alpha} = a^2 + 2ab\sqrt{6} + 6b^2$. $Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}) = 2(a^2 + 6b^2)$*

e $t_{\mathcal{O}_K} = \min\{Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}); \alpha \in \mathcal{O}_K, \alpha \neq 0\} = 2 (a = 1 \text{ e } b = 0)$. Portanto

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{4\sqrt{6}} \approx 0,1020.$$

Consideremos ideais principais do anel dos inteiros algébricos de um corpo quadrático K .

Seja $\mathfrak{a}$ um ideal principal não nulo de $\mathcal{O}_K$, $\mathfrak{a} = \gamma\mathcal{O}_K$. Então $\sigma_K(\mathfrak{a})$ é um reticulado de posto 2 em $\mathbb{R}^2$ e sua densidade de centro, pela Observação 2.1, vale:

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

Exemplo 3.2 Sejam $K = \mathbb{Q}(\sqrt{10})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{10}]$ e $\mathfrak{a}$ o ideal principal de $\mathcal{O}_K$, gerado por $\gamma = 1 + 2\sqrt{10}$. Dado $\alpha \in \gamma\mathcal{O}_K$ existem $a, b \in \mathbb{Z}$ tais que

$$\alpha = (a + 20b) + (2a + b)\sqrt{10}.$$

Logo

$$\alpha\bar{\alpha} = (a + 20b)^2 + 10(2a + b)^2 + 2.(a + 20b)(2a + b)\sqrt{10}$$

e

$$Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}) = 2[(a + 20b)^2 + 10(b + 2a)^2].$$

Assim $t_{\mathfrak{a}} = \min\{Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}); \alpha \in \mathfrak{a}, \alpha \neq 0\} = 82 (a = 1 \text{ e } b = 0)$. Sendo $\mathfrak{D}_K = 40$ e $N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(\gamma)| = 39$ temos

$$\delta(\sigma_K(\mathfrak{a})) = \frac{41}{156\sqrt{10}} \approx 0,0831.$$

Exemplo 3.3 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 $\gamma = 3 - 2\sqrt{5}$. Dado $\alpha \in \gamma\mathcal{O}_K$ existem $a, b \in \mathbb{Z}$ tais que

$$\alpha = (3a - \frac{7}{2}b) + (-2a + \frac{1}{2}b)\sqrt{5}.$$

Logo

$$\alpha\bar{\alpha} = (3a - \frac{7}{2}b)^2 + (-2a + \frac{1}{2}b)^2 5 + 2(3a - \frac{7}{2}b)(-2a + \frac{1}{2}b)\sqrt{5} \text{ e}$$

$$Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}) = 2[(3a - \frac{7}{2}b)^2 + 5(-2a + \frac{1}{2}b)^2].$$

Atribuindo valores inteiros para a e b não todos nulos, concluímos que $t_{\mathfrak{a}} = \min\{Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}); \alpha \in \mathfrak{a}, \alpha \neq 0\} = 27$ ($a = 0$ e $b = 1$). Sendo $\mathfrak{D}_K = 5$ e $|N_{K/\mathbb{Q}}(\gamma)| = 11$ temos

$$\delta(\sigma_K(\mathfrak{a})) = \frac{27}{44\sqrt{5}} \approx 0,2744.$$

Exemplo 3.4 Sejam $K = \mathbb{Q}(\sqrt{-3})$, $\mathcal{O}_K = \mathbb{Z}[w]$ e $\alpha = a + bw \in \mathcal{O}_K$, com $w = \frac{1+\sqrt{-3}}{2}$. Então $\alpha\bar{\alpha} = a^2 + ab + b^2$, $Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}) = 2(a^2 + ab + b^2)$ e $t_{\mathcal{O}_K} = \min\{Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}); \alpha \in \mathcal{O}_K, \alpha \neq 0\} = 2$ ($a = 0$ e $b = 1$). Visto que $\mathfrak{D}_K = -3$, temos

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{2\sqrt{3}} \approx 0,2886.$$

Afirmção: 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 de $\sigma_K(\mathfrak{a})$ é a mesma de $\sigma_K(\mathcal{O}_K)$. De fato, sejam $\mathfrak{a} = \alpha\mathcal{O}_K$ um ideal principal de $\mathcal{O}_K$ e $x \in \mathfrak{a}$, $x = \alpha l$; $l \in \mathcal{O}_K$, então $x\bar{x} = \alpha\bar{\alpha}l\bar{l}$ e $Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}l\bar{l}) = 2(\alpha\bar{\alpha}l\bar{l})$. Mas

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

logo, $\rho_{\alpha\mathcal{O}_K} = |N(\alpha)| \cdot \rho_{\mathcal{O}_K}$ e, portanto,

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

3.2 Reticulados em Corpos Ciclotômicos

Dado um inteiro n , seja $Q_n(\underline{X})$ a forma quadrática definida por

$$Q_n(\underline{X}) = Q_n(X_1, \dots, X_n) = \sum_{i=1}^n X_i^2 + \sum_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

Note que $Q_n(\underline{X})$ é positiva definida, simétrica e $Q_n(-v) = Q_n(v)$; $v \in \mathbb{R}^n$.

Teorema 3.1 [1]

1. Dados $a_1, \dots, a_r$ números inteiros, com $r < n$, seja

$$F(X_{r+1}, \dots, X_n) = Q_n(a_1, \dots, a_r, X_{r+1}, \dots, X_n).$$

Então o menor valor que F assume, com entradas inteiras, é em

$$(y, y, \dots, y), \text{ sendo } y = \left\lfloor \frac{\sum_{i=1}^r a_i}{r+1} \right\rfloor$$

e $\lfloor z \rfloor$ denota o inteiro mais próximo de z .

2. Seja $H : \mathbb{N} \rightarrow \mathbb{R}$ definida por

$$H(a) = \min \{ Q(a, a_2, \dots, a_n); (a_2, \dots, a_n) \in \mathbb{Z}^{n-1} \}.$$

Então

$$H(a) = \begin{cases} (n+1) \cdot \left(\frac{a^2}{2}\right) & \text{se } a \text{ é par} \\ (n+1) \cdot \left(\frac{a^2+1}{2}\right) - 1 & \text{se } a \text{ é ímpar.} \end{cases}$$

A função H acima definida é crescente, logo o menor valor que $Q_n(\underline{X})$ assume é n , quando $a = 1$.

Sejam p um número primo, $K = \mathbb{Q}(\xi_p)$ e $\alpha = \sum_{i=0}^{p-2} a_i \xi_p^i \in \mathbb{Z}[\xi_p]$. Sendo

$$\overline{\xi_p} = \xi_p^{-1} \text{ temos } \overline{\alpha} = \sum_{i=0}^{p-2} a_i \xi_p^{-i} \text{ e}$$

$$\begin{aligned} \alpha \overline{\alpha} &= \left(\sum_{i=0}^{p-2} a_i \xi_p^i \right) \cdot \left(\sum_{i=0}^{p-2} a_i \xi_p^{-i} \right) \\ &= (a_0^2 + \dots + a_{p-2}^2) + (a_0 a_1 + \dots + a_{p-3} a_{p-2})(\xi_p + \xi_p^{-1}) + \dots \\ &\quad \dots + (a_0 a_{p-3} + a_1 a_{p-2})(\xi_p^{p-3} + \xi_p^{-(p-3)}) + a_0 a_{p-2}(\xi_p^{p-2} + \xi_p^{-(p-2)}) \end{aligned}$$



Por outro lado, fazendo $\alpha_i = \xi_p^i + \xi_p^{-i}$ e $A_i = a_0 a_i + a_1 a_{i+1} + \dots + a_{p-2-i} a_{p-2}$, temos $\alpha \bar{\alpha} = A_0 + A_1 \alpha_1 + \dots + A_{p-2} \alpha_{p-2}$. Mas $Tr_{K/\mathbb{Q}}(\alpha_i) = -2$ então

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha}) &= (p-1)A_0 - 2(A_1 + A_2 + \dots + A_{p-2}) \\ &= (p-1)A_0 - 2(a_0 a_1 + \dots + a_{p-3} a_{p-2} + a_0 a_2 + \dots + a_{p-4} a_{p-2} + \\ &\quad + \dots + a_0 a_{p-3} + a_1 a_{p-2} + a_0 a_{p-2}) \end{aligned}$$

logo,

$$Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha}) = p \sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i^2 + 2 \sum_{0 \leq i < j \leq p-2} a_i a_j \right]$$

e, portanto,

$$Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha}) = p \sum_{i=0}^{p-2} a_i^2 - \left[\sum_{i=0}^{p-2} a_i \right]^2. \quad (3.1)$$

Entretanto, fazendo algumas operações simples com o segundo membro da Igualdade 3.1, podemos apresentar $Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha})$ em duas outras maneiras:

$$Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha}) = \sum_{i=0}^{p-2} a_i^2 + \sum_{0 \leq i < j \leq p-2} (a_i - a_j)^2 \quad (3.2)$$

e

$$Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha}) = d^2(P, 0) + (p-1)d^2(P, \Delta), \quad (3.3)$$

sendo $P = (a_0, \dots, a_{p-2})$ e $d^2(P, 0)$ o quadrado da distância euclidiana de P até a origem e $d^2(P, \Delta)$ o quadrado da distância euclidiana de P até a diagonal de $\mathbb{R}^{p-1}$.

Podemos verificar que a Expressão 3.2 é a imagem da forma quadrática $Q_{p-1}(\underline{X})$ calculada em $(a_0, \dots, a_{p-2})$.

Portanto, quando $K = \mathbb{Q}(\xi_p)$

$$t_{\mathcal{O}_K} = \min\{Tr_{K/\mathbb{Q}}(\alpha \bar{\alpha}); \alpha \in \mathcal{O}_K, \alpha \neq 0\} = p-1.$$

Vamos considerar ideais principais não nulos do anel dos inteiros algébricos de um corpo ciclotômico e calcular sua densidade de centro.

Com a notação acima, seja $\mathfrak{p} = \lambda \mathcal{O}_K$ o ideal primo de $\mathcal{O}_K$, com $\lambda = 1 - \xi_p$. Dado $\alpha \in \mathfrak{p}$, $\alpha = \sum_{i=0}^{p-2} a_i \xi_p^i$ tem-se $\alpha \equiv \sum_{i=0}^{p-2} a_i \pmod{\mathfrak{p}}$, pois $\xi_p \equiv 1 \pmod{\mathfrak{p}}$. Então $\alpha \in \mathfrak{p}$ se, e somente se, $\sum_{i=0}^{p-2} a_i \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Visto que $1 - \xi_p \in \mathfrak{p}$ e $Q(1, -1, 0, \dots, 0) = 2p$ então

$$t_{\mathfrak{p}} = \min\{Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}); \alpha \in \mathfrak{p}, \alpha \neq 0\} = 2p.$$

Visto que $N(\mathfrak{p}) = N(\lambda) = p$ e $\mathfrak{D}_K = \pm p^{p-2}$ então

$$\delta(\sigma_K(\mathfrak{p})) = \frac{\left(\frac{2p}{4}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}} \cdot p} = \frac{p^{\frac{p-1}{2}}}{2^{\frac{p-1}{2}} \cdot p^{\frac{p}{2}}} = \frac{1}{p^{\frac{1}{2}} \cdot 2^{\frac{p-1}{2}}}.$$

No caso do anel, temos

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{(p-1)^{\frac{p-1}{2}}}{2^{p-1} \cdot p^{\frac{p-2}{2}}}.$$

Quando $p = 3$, temos

$$\delta(\sigma_K(\mathfrak{p})) = \frac{1}{2\sqrt{3}} \approx 0,2886$$

e $p = 5$, temos

$$\delta(\sigma_K(\mathfrak{p})) = \frac{1}{4\sqrt{5}} \approx 0,1118.$$

Passaremos a calcular a densidade de centro de $\sigma_K(\mathfrak{p}^i)$, $i \geq 1$.

Dadas as condições para um elemento de $\mathcal{O}_K$ pertencer ao ideal $\mathfrak{p}^i$, precisamos encontrar o mínimo que a forma quadrática assume nos elementos de $\mathfrak{p}^i$ para, efetivamente, calcular a densidade de centro de $\sigma_K(\mathfrak{p}^i)$.

Teorema 3.2 [2] *Sejam $K = \mathbb{Q}(\xi_p)$ e $\mathfrak{p} = (1 - \xi_p)\mathcal{O}_K$. Se $\alpha \in \mathfrak{p}^i$, $i = 1, \dots, \frac{p-1}{2}$; então $Tr_{K/\mathbb{Q}}(\alpha\bar{\alpha}) \geq 2 \cdot p \cdot i$.*



Pelo Teorema acima e pelo fato da norma ser multiplicativa, temos:

$$\delta(\sigma_K(p^i)) \geq \frac{\left(\frac{p \cdot i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2}{2}} \cdot p^i} = \frac{p^{\frac{p-1}{2}} \cdot \left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2+2i}{2}}} = \frac{\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{\frac{p-2+2i}{2}} \cdot p^{\frac{1-p}{2}}} = \frac{\left(\frac{i}{2}\right)^{\frac{p-1}{2}}}{p^{i-\frac{1}{2}}}.$$

A última expressão acima é maximizada, via derivação, no valor $\frac{p-1}{2 \ln p}$ para i . Evidentemente deveremos tomar i como sendo um número inteiro próximo de $\frac{p-1}{2 \ln p}$.

Para $p = 5$ temos $\frac{p-1}{2 \ln p} \approx 1,24$ e $i = 1$ já conhecemos e quando $i = 2$ temos

$$\delta(\sigma_K(p^2)) = \frac{\left(\frac{2}{2}\right)^2}{5^{\frac{3}{2}}} = \frac{1}{5\sqrt{5}} \approx 0,0894.$$

3.3 Cúbicas não Galoisianas

Nesta Seção damos início ao estudos de casos particulares de cúbicas, com o objetivo de obter reticulados de posto 3 em $\mathbb{R}^3$.

Devido à complexidade do caso geral, aqui enfocaremos as cúbicas da forma $\mathbb{Q}(\sqrt[3]{d})$ sendo d um número inteiro livre de quadrados.

Os objetivos aqui são a determinação do anel dos inteiros algébricos de $K = \mathbb{Q}(\sqrt[3]{d})$, o discriminante de K , a forma quadrática associada e a descrição dos reticulados obtidos em $\mathbb{R}^3$ a partir de ideais ordinários de $\mathcal{O}_K$.

Para atingir tais metas, faremos uso do Lema de Kummer e de demais tópicos da Teoria Algébrica dos Números, desenvolvidas nos capítulos anteriores.

Sejam d um inteiro livre de quadrados, $\theta = \sqrt[3]{d}$, $K = \mathbb{Q}(\theta)$ 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 $a_0, a_1, a_2 \in \mathbb{Q}$ tais que $\alpha = a_0 + a_1\theta + a_2\theta^2$. O polinômio



$\text{irr}(\theta, \mathbb{Q})$ é $X^3 - d$ e suas raízes são $\theta, \theta\xi_3, \theta\xi_3^2$ e $X^2 + X + 1 = \text{irr}(\xi_3, \mathbb{Q})$. Sejam $\sigma_1, \sigma_2, \sigma_3$ os monomorfismos de K em $\mathbb{C}$ tal que σ_1 é a inclusão, $\sigma_2(\theta) = \theta\xi_3$ e $\sigma_3(\theta) = \theta\xi_3^2$.

Dado $\alpha \in K$, se $\alpha_i = \sigma_i(\theta)$; $i = 1, 2, 3$ então o polinômio característico de α é:

$$\begin{aligned} f_\alpha(X) &= (X - \alpha_1)(X - \alpha_2)(X - \alpha_3) \\ &= X^3 - X^2(\alpha_1 + \alpha_2 + \alpha_3) + X(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - \alpha_1\alpha_2\alpha_3 \end{aligned}$$

Fazendo os cálculos e respectivas substituições, obtemos

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 3a_0, \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= 3a_0^2 - 3a_1a_2d, \\ \alpha_1\alpha_2\alpha_3 &= a_0^3 - 3a_0a_1a_2d + d(a_1^3 + a_2^3d). \end{aligned}$$

Portanto

$$f_\alpha(X) = X^3 - 3a_0X^2 + (3a_0^2 - 3a_1a_2d)X - [a_0^3 - 3a_0a_1a_2d + d(a_1^3 + a_2^3d)].$$

Da definição de elemento inteiro, tem-se:

$$\alpha \in \mathcal{O}_K \Leftrightarrow \begin{cases} 3a_0 \in \mathbb{Z} \\ 3a_0^2 - 3a_1a_2d \in \mathbb{Z} \\ a_0^3 - 3a_0a_1a_2d + d(a_1^3 + a_2^3d) \in \mathbb{Z}. \end{cases}$$

Afirmção. $\theta\mathcal{O}_K \cap \mathbb{Z} = d\mathbb{Z}$. De fato, $d \in \mathbb{Z}$ e $d \in \theta\mathcal{O}_K$ então $d \in \theta\mathcal{O}_K \cap \mathbb{Z}$, logo $d\mathbb{Z} \subset \theta\mathcal{O}_K \cap \mathbb{Z}$. Seja $\theta\gamma \in \theta\mathcal{O}_K \cap \mathbb{Z}$ então existe n tal que $\theta\gamma = n$. Aplicando a norma, obtemos

$$N(\theta\gamma) = \theta^3 N(\gamma) = dN(\gamma) = n^3,$$

o que implica d divide n^3 , mas d é inteiro livre de quadrados, então d divide n . Logo $\theta\gamma \in d\mathbb{Z}$ e, portanto, $\theta\mathcal{O}_K \cap \mathbb{Z} = d\mathbb{Z}$. Por outro lado,

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\theta\gamma) &= \sigma_1(\theta\gamma) + \sigma_2(\theta\gamma) + \sigma_3(\theta\gamma) = \theta\sigma_1(\gamma) + \theta\xi_3\sigma_2(\gamma) + \theta\xi_3^2\sigma_3(\gamma) \\ &= \theta(\sigma_1(\gamma) + \xi_3\sigma_2(\gamma) + \xi_3^2\sigma_3(\gamma)) = \theta w \end{aligned}$$

e visto que o traço de um elemento inteiro algébrico é sempre um número inteiro então $\theta w = m$; $m \in \mathbb{Z}$, e assim $w = \frac{m}{\theta} \in K$. Além disso,

$$\begin{aligned} Tr_{K/\mathbb{Q}}(\alpha\theta) &= Tr_{K/\mathbb{Q}}(a_0\theta + a_1\theta^2 + a_2d) = 3a_2d \in d\mathbb{Z}, \\ Tr_{K/\mathbb{Q}}(\alpha\theta^2) &= Tr_{K/\mathbb{Q}}(a_0\theta^2 + a_1d + \theta d) = 3a_1d \in d\mathbb{Z}, \end{aligned}$$

logo $3a_0, 3a_1, 3a_2 \in \mathbb{Z}$ e, conseqüentemente, podemos supor

$$\alpha = \frac{b_0}{3} + \frac{b_1}{3}\theta + \frac{b_2}{3}\theta^2 \in \mathcal{O}_K, b_i \in \mathbb{Z}; i = 1, 2, 3.$$

Logo

$$\alpha = c_0 + c_1\theta + c_2\theta^2 + \frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2;$$

com $c_i \in \mathbb{Z}$ e $r_i \in \{0, \pm 1\}$, $i = 1, 2, 3$. Visto que α é inteiro algébrico se, e somente se, $\frac{r_0}{3} + \frac{r_1}{3}\theta + \frac{r_2}{3}\theta^2$ também o é, podemos concluir que:

$$\alpha \in \mathcal{O}_K \Leftrightarrow \begin{cases} r_0 \in \mathbb{Z} \\ 3[(\frac{r_0}{3})^2 - \frac{r_1}{3} \cdot \frac{r_2}{3}d] \in \mathbb{Z} \\ (\frac{r_0}{3})^3 - 3\frac{r_0}{3} \cdot \frac{r_1}{3} \cdot \frac{r_2}{3}d + d[(\frac{r_1}{3})^3 + (\frac{r_2}{3})^3d] \in \mathbb{Z} \end{cases}$$

ou seja,

$$\begin{cases} \frac{(r_0)^2 - r_1 r_2 d}{3} \in \mathbb{Z} \\ \frac{(r_0)^3 - 3r_0 r_1 r_2 d + d[(r_1)^3 + d(r_2)^3]}{27} \in \mathbb{Z} . \end{cases}$$

Agora analisemos todas as possibilidades para $r_i \in \{0, \pm 1\}$.

r_0	r_1	r_2	$\frac{(r_0)^2 - r_1 r_2 d}{3}$	$\frac{(r_0)^3 - 3r_0 r_1 r_2 d + d[(r_1)^3 + d(r_2)^3]}{27}$	$d \pmod{9}$
0	0	0	0	0	$\forall d$
1	1	1	$\frac{1-d}{3}$	$\frac{(d-1)^2}{27}$	$d \equiv 1$
1	1	-1	$\frac{1+d}{3}$	$\frac{(-d^2+4d+1)}{27}$	$\nexists d$
1	-1	1	$\frac{1+d}{3}$	$\frac{(d+1)^2}{27}$	$d \equiv -1$
1	-1	-1	$\frac{1-d}{3}$	$\frac{(-d^2-4d+1)}{27}$	$\nexists d$
-1	1	1	$\frac{1-d}{3}$	$\frac{(d^2+4d-1)}{27}$	$\nexists d$
-1	1	-1	$\frac{1+d}{3}$	$\frac{-(d+1)^2}{27}$	$d \equiv -1$
-1	-1	1	$\frac{1+d}{3}$	$\frac{(d^2-4d-1)}{27}$	$\nexists d$
-1	-1	-1	$\frac{1-d}{3}$	$\frac{-(d-1)^2}{27}$	$d \equiv 1$

Da tabela acima temos o seguinte

Teorema 3.3 *Sejam d um inteiro livre de quadrados, $\theta = \sqrt[3]{d}$, $K = \mathbb{Q}(\theta)$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . Então*

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

com $\omega = \frac{1+\theta+\theta^2}{3}$ e $\gamma = \frac{1-\theta+\theta^2}{3}$.

Sejam d um inteiro livre de quadrados, $\theta = \sqrt[3]{d}$, $K = \mathbb{Q}(\sqrt[3]{d})$ e $\mathcal{O}_K$ o anel dos inteiros algébricos de K . Dado $\alpha \in K$, $\alpha = a + b\theta + c\theta^2$ e visto que $r_2 = 1$ o homomorfismo canônico σ_K de K em $\mathbb{R}^3$ é dado por $\sigma_K(\alpha) = (\alpha, R\sigma_2(\alpha), I\sigma_2(\alpha))$ e, portanto,



$$\begin{aligned}
|\sigma_K(\alpha)|^2 &= \alpha^2 + \sigma_2(\alpha)\overline{\sigma}_2(\alpha) = \alpha^2 + \sigma_2(\alpha)\sigma_2(\overline{\alpha}) \\
&= (a + b\theta + c\theta^2)^2 + (a + b\theta\xi_3 + c\theta^2\xi_3^2)(a + b\theta\xi_3^2 + c\theta^2\xi_3) \\
&= 2a^2 + 2b^2\theta^2 + 2c^2\theta^4 + ab\theta + bcd + ac\theta^2 \\
&= 2a^2 + 2(b\theta)^2 + 2(c\theta^2)^2 + a(b\theta) + (b\theta)(c\theta^2) + a(c\theta^2) \\
&= \frac{1}{2}\{2a^2 + 2(b\theta)^2 + 2(c\theta^2)^2 + (a + b\theta)^2 + (b\theta + c\theta^2)^2 + (a + c\theta^2)\}
\end{aligned}$$

A forma quadrática é minimizada em $a = 1, b = c = 0$, assumindo o valor 2, logo $\rho = \frac{\sqrt{2}}{2}$. Visto que $\mathfrak{D}_K = \pm N(f'(\theta)) = \pm 27.d^2$ então a densidade de centro de $\sigma_K(\mathcal{O}_K)$ é

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{2.(\sqrt{2}/2)^3}{\sqrt{27d^2}} = \frac{1}{3\sqrt{6}.d}.$$

Quando $d = 2$, temos

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{1}{6\sqrt{6}} \approx 0,0680.$$

Exemplo 3.5 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$, $\mathbb{Z}[\sqrt[3]{2}]$ 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:

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

e pelo Lema de Kummer, $3\mathcal{O}_K = \mathfrak{p}^3$, $\mathfrak{p} = (3, \theta + 1)$ sendo o único ideal primo de $\mathcal{O}_K$ acima de $3\mathbb{Z}$, cujo grau residual é 1 e a norma é 3. Além disso, $r_2 = 1$ e $\mathfrak{D}_K = \pm 27.4$. Assim para calcular a densidade de centro do ideal primo $\sigma_K(\mathfrak{p})$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, $\alpha = a + b\theta + c\theta^2$ e como $\mathfrak{p}$ está acima de $3\mathbb{Z}$ e $\theta \equiv -1 \pmod{\mathfrak{p}}$ então $\alpha \in \mathfrak{p}$ se, e somente se, $a - b + c \in \mathfrak{p} \cap \mathbb{Z} = 3\mathbb{Z}$. Nosso próximo passo é minimizar a forma quadrática

$$|\sigma_K(\alpha)|^2 = \frac{1}{2}\{2a^2 + 2(b\theta)^2 + 2(c\theta^2)^2 + (a + b\theta)^2 + (a + c\theta^2)^2 + (b\theta + c\theta^2)^2\},$$

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

$$\rho = \frac{\sqrt{-\theta^2 + 4\theta + 2}}{2}$$

e

$$\delta(\sigma_K(\mathfrak{p})) = \frac{2 \cdot (\sqrt{-\theta^2 + 4\theta + 2}/2)^3}{6 \cdot \sqrt{3} \cdot 3} = \frac{(\sqrt{-\theta^2 + 4\theta + 2})^3}{8 \cdot 9 \cdot \sqrt{3}} = 0,1021.$$

Exemplo 3.6 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$, $\mathbb{Z}[\sqrt[3]{2}]$ o anel dos inteiros algébricos de K e $X^3 - 2$ o polinômio irredutível de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Consideremos o ideal $5\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^3 - 2$ fatora-se como:

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

e pelo Lema de Kummer, $5\mathcal{O}_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$, sendo

$$\mathfrak{p}_1 = (5, \theta - 3) \quad \text{e} \quad \mathfrak{p}_2 = (5, \theta^2 + 3\theta - 1)$$

os ideais primos de $\mathcal{O}_K$ acima de $5\mathbb{Z}$, cujos graus residuais são 1 e 2, respectivamente. Além disso $N(\mathfrak{p}_1) = 5$, $N(\mathfrak{p}_2) = 5^2$, $r_2 = 1$ e $\mathfrak{D}_K = \pm 27.4$. Assim para calcular a densidade de centro do ideal primo $\sigma_K(\mathfrak{p}_1)$, precisamos apenas determinar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, $\alpha = a + b\theta + c\theta^2$ e como $\mathfrak{p}_1$ está acima de $5\mathbb{Z}$ e $\theta \equiv 3 \pmod{\mathfrak{p}_1}$ então $\alpha \in \mathfrak{p}_1$ se, e somente se, $a - 2b - c \in \mathfrak{p}_1 \cap \mathbb{Z} = 5\mathbb{Z}$. Precisamos então minimizar a forma quadrática

$$|\sigma_K(\alpha)|^2 = \frac{1}{2} \{2a^2 + 2(b\theta)^2 + 2(c\theta^2)^2 + (a + b\theta)^2 + (a + c\theta^2)^2 + (b\theta + c\theta^2)^2\},$$

para valores de $a, b, c \in \mathbb{Z}$ que satisfazem a condição $a - 2b - c \in 5\mathbb{Z}$. Analizando todas as possibilidades, temos que a forma quadrática $|\sigma_K(\alpha)|^2$

assume seu valor mínimo quando $a = 1$, $b = 1$ e $c = -1$ e este valor é $\theta^2 + 5\theta$.

Logo,

$$\rho = \frac{\sqrt{\theta^2 + 5\theta}}{2}$$

e

$$\delta(\sigma_K(\mathfrak{p}_1)) = \frac{2.(\sqrt{\theta^2 + 5\theta}/2)^3}{6.\sqrt{3}.5} = \frac{(\sqrt{\theta^2 + 5\theta})^3}{120.\sqrt{3}} = 0,1066.$$

Exemplo 3.7 Sejam $K = \mathbb{Q}(\theta)$, $\theta = \sqrt[3]{2}$, $\mathbb{Z}[\sqrt[3]{2}]$ o anel dos inteiros algébricos de K e $X^3 - 2$ o polinômio irredutível de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Consideremos o ideal $2\mathbb{Z} \subset \mathbb{Z}$. O polinômio $X^3 - 2$ fatora-se como:

$$X^3 - 2 \equiv X^3 \pmod{2\mathbb{Z}[X]}$$

e, pelo Lema de Kummer, $2\mathcal{O}_K = \mathfrak{p}^3$, $\mathfrak{p} = (2, \theta)$ sendo o único ideal primo de $\mathcal{O}_K$ acima de $2\mathbb{Z}$, cujo grau residual é 1 e a norma é 2. Além disso, $r_2 = 1$ e $\mathfrak{D}_K = \pm 27.4$. Assim para calcular a densidade de centro do ideal primo $\sigma_K(\mathfrak{p})$, precisamos apenas encontrar o raio de empacotamento. Dado $\alpha \in \mathcal{O}_K$, $\alpha = a + b\theta + c\theta^2$ e como $\mathfrak{p}$ está acima de $2\mathbb{Z}$ e $\theta \equiv 0 \pmod{\mathfrak{p}}$ então $\alpha \in \mathfrak{p}$ se, e somente se, $a \in \mathfrak{p} \cap \mathbb{Z} = 2\mathbb{Z}$. Nosso próximo passo é minimizar a forma quadrática

$$|\sigma_K(\alpha)|^2 = \frac{1}{2} \{2a^2 + 2(b\theta)^2 + 2(c\theta^2)^2 + (a + b\theta)^2 + (a + c\theta^2)^2 + (b\theta + c\theta^2)^2\},$$

para valores de $a, b, c \in \mathbb{Z}$ que satisfazem a condição $a \in 2\mathbb{Z}$. Neste caso a forma quadrática $|\sigma_K(\alpha)|^2$ assume seu valor mínimo quando $a = 0$, $b = 1$ e $c = 0$ e este valor é $2\theta^2$. Logo,

$$\rho = \frac{\sqrt{2\theta^2}}{2} = \frac{\theta}{\sqrt{2}}$$

e

$$\delta(\sigma_K(\mathfrak{p})) = \frac{2.(\frac{\theta}{\sqrt{2}})^3}{6.\sqrt{3}.2} = \frac{2}{12.\sqrt{6}} = \frac{1}{6.\sqrt{6}} \approx 0,0680.$$

3.4 Cúbicas Galoisianas

Na Seção anterior estudamos apenas as cúbicas não galoisianas da forma $\mathbb{Q}(\sqrt[3]{d})$, d um inteiro livre de quadrados e na presente Seção nosso enfoque será as cúbicas galoisianas, que pelo Teorema de Kronecker-Weber estão contidas em algum corpo do tipo $\mathbb{Q}(\xi_n)$.

Os objetivos aqui são a determinação do anel dos inteiros algébricos da cúbica galoisiana, seu discriminante, a forma quadrática associada e a descrição dos reticulados obtidos em $\mathbb{R}^3$ a partir de ideais ordinários, com ênfase para o cálculo da densidade de centro.

Para tanto, faremos uso da Teoria de Galois e outros tópicos da Teoria Algébrica dos Números, desenvolvidas nos capítulos anteriores.

Tendo em vista a complexidade do caso geral, restringiremos o nosso interesse aos corpos $\mathbb{Q}(\xi_{p^r})$, p primo, $r \geq 1$.

Lema 3.1 *Sejam p um número primo, $r \geq 1$ e L o corpo ciclotômico $\mathbb{Q}(\xi_{p^r})$ de grau $(p-1)p^{r-1}$. Então L contém uma cúbica se, e somente se, 3 divide $(p-1)p^{r-1}$.*

Demonstração. Visto que o grupo de Galois de $\mathbb{Q}(\xi_{p^r})$ sobre $\mathbb{Q}$, G é isomorfo ao grupo cíclico $(\frac{\mathbb{Z}}{p^r\mathbb{Z}})^*$ de ordem $(p-1)p^{r-1}$ então, da Teoria de Grupos Finitos, dado d um divisor de $(p-1)p^{r-1}$, existe um único subgrupo H de G ; de ordem d . Em particular se 3 divide $(p-1)p^{r-1}$ existe um subgrupo H de G de ordem 3 o qual fixará a cúbica contida em $\mathbb{Q}(\xi_{p^r})$. $\square$

A condição 3 divide $(p-1)p^{r-1}$ é satisfeita quando 3 divide $p-1$ ou $p=3$ e $r > 1$.

No caso $p=3$ e $r > 1$, pelo Lema 3.1, é suficiente estudar a cúbica contida em $\mathbb{Q}(\xi_9)$.



Exemplo 3.8 Dado $L = \mathbb{Q}(\xi_9)$ a única cúbica contida em L é $K = \mathbb{Q}(\theta)$ com $\theta = \xi_9 + \xi_9^{-1}$. Mostremos que o anel $\mathcal{O}_K$ é $\mathbb{Z}[\theta]$. Temos $\mathbb{Z}[\theta] \subset \mathcal{O}_K$ e por outro lado, $\mathcal{O}_K \subset \mathbb{Q}(\theta)$ logo existem $a, b, c \in \mathbb{Q}$ tais que

$$\begin{aligned}\alpha &= a + b\theta + c\theta^2 \\ &= a + b(\xi_9 + \xi_9^{-1}) + c(\xi_9 + \xi_9^{-1})^2 \\ &= a + b(\xi_9 + \xi_9^{-1}) + c(\xi_9^2 + \xi_9^{-2} + 2).\end{aligned}$$

Sendo $\text{irr}(\xi_9, \mathbb{Q}) = X^6 + X^3 + 1$ então $\xi_9^{-1} = -\xi_9^5 - \xi_9^2$ e $\xi_9^{-2} = -\xi_9^4 - \xi_9$. Portanto $\alpha = (a + 2c) + (b - c)\xi_9 + (c - b)\xi_9^2 - c\xi_9^4 - b\xi_9^5$.

Visto que $\theta \in \mathcal{O}_K \subset \mathcal{O}_L$ e $\{1, \xi_9, \dots, \xi_9^5\}$ é base integral de $\mathcal{O}_L$ então temos $a, b, c \in \mathbb{Z}$ e, portanto, $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Sendo $\theta = \xi_9 + \xi_9^{-1}$, temos $f(X) = X^3 - 3X + 1 = \text{irr}(\theta, \mathbb{Q})$. Dado $\gamma = a + b\theta + c\theta^2 \in K$ o homomorfismo canônico σ_K de K em $\mathbb{R}^3$ é dado por $\sigma_K(\gamma) = (\sigma_1(\gamma), \sigma_2(\gamma), \sigma_4(\gamma))$ e, conseqüentemente,

$$\begin{aligned}|\sigma_K(\gamma)|^2 &= \text{Tr}_{K/\mathbb{Q}}(\gamma\bar{\gamma}) = \text{Tr}_{K/\mathbb{Q}}(\gamma^2) = 3(a^2 + 4ac + 6c^2 + 2b^2 - 2bc) \\ &= 3[(a + 2c)^2 + (-b + c)^2 + b^2 + c^2].\end{aligned}$$

Atribuindo valores inteiros para a, b e c temos que a forma quadrática $|\sigma_K(\gamma)|^2$ assume o valor mínimo 3, quando $a = 1, b = c = 0$ e assim $\rho = \frac{\sqrt{3}}{2}$. Pelo Teorema 2.5, $\mathfrak{D}_K = \pm 81$ portanto

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{\sqrt{3}}{24} \approx 0,0722.$$

Exemplo 3.9 Seja $\mathfrak{p}$ o ideal principal de $\mathcal{O}_K$ gerado por $(2 - \theta)$. Dado $\alpha = a + b\theta + c\theta^2 \in \mathcal{O}_K$ e visto que $\mathfrak{p}$ está acima de $3\mathbb{Z}$ e $\theta \equiv 2 \pmod{\mathfrak{p}}$ então $\alpha \in \mathfrak{p}$ se, e somente se, $a - b + c \in 3\mathbb{Z}$. Atribuindo valores inteiros para a, b e c temos que a forma quadrática

$$|\sigma_K(\alpha)|^2 = 3[(a + 2c)^2 + (-b + c)^2 + b^2 + c^2]$$

assume o valor mínimo 9 em $a = b = 1$ e $c = 0$, logo $\rho = \frac{3}{2}$. Visto que $N(\mathfrak{p}) = 3$ e $\mathfrak{D}_K = \pm 81$ temos

$$\delta(\sigma_K(\mathfrak{p})) = \frac{\left(\frac{3}{2}\right)^3}{9 \cdot 3} = \frac{1}{8} \approx 0,125.$$

Quando $p \equiv 1 \pmod{3}$ é suficiente estudar $\mathbb{Q}(\xi_p)$, pois a cúbica contida em $\mathbb{Q}(\xi_{p^r})$ está contida em $\mathbb{Q}(\xi_p)$. Nestas condições existem infinitos números primos, devido ao Teorema de Dirichlet para primos em Progressão Aritmética.

Sejam p um número primo, $L = \mathbb{Q}(\xi_p)$, $\mathbb{Z}(\xi_p)$ o anel dos inteiros algébricos de L e $K \subset \mathbb{Q}(\xi_p)$, $[K : \mathbb{Q}] = 3$. Pelo Teorema 2.6, $K = \mathbb{Q}(\theta)$, $\theta = \text{Tr}_{L/K}(\xi_p)$ e $\mathcal{O}_K = \mathbb{Z}\theta + \mathbb{Z}\sigma(\theta) + \mathbb{Z}\sigma^2(\theta)$, com $\{Id_K, \sigma, \sigma^2\} = \text{Gal}(K/\mathbb{Q})$.

Seja $\alpha = a_0\theta + a_1\sigma(\theta) + a_2\sigma^2(\theta) \in \mathcal{O}_K$. Sendo K um corpo real e σ_K o homomorfismo canônico de K em $\mathbb{R}^3$, temos: $\sigma_K(\alpha) = (\alpha, \sigma(\alpha), \sigma^2(\alpha))$ e

$$|\sigma_K(\alpha)|^2 = (a_0^2 + a_1^2 + a_2^2) + \left(\frac{p-1}{3}\right)[(a_0 - a_1)^2 + (a_0 - a_2)^2 + (a_1 - a_2)^2].$$

O menor valor que a forma quadrática acima assume é 3, quando $a_0 = a_1 = a_2 = 1$. Logo $\rho = \frac{\sqrt{3}}{2}$ e visto que $\mathfrak{D}_K = \pm p^{[K:\mathbb{Q}]-1} = \pm p^2$ temos

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{\left(\frac{\sqrt{3}}{2}\right)^3}{p} = \frac{3\sqrt{3}}{8 \cdot p}.$$

No caso $p = 7$, temos

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{\left(\frac{\sqrt{3}}{2}\right)^3}{7} = \frac{3\sqrt{3}}{56} \approx 0,0926$$

e quando $p = 13$, temos

$$\delta(\sigma_K(\mathcal{O}_K)) = \frac{\left(\frac{\sqrt{3}}{2}\right)^3}{13} = \frac{3\sqrt{3}}{104} \approx 0,0500.$$

Exemplo 3.10 Sejam K uma cúbica contida em $\mathbb{Q}(\xi_p)$ e $\mathcal{O}_K$ o anel dos inteiros de K . Dado o ideal $\mathfrak{p}_K = (1 - \xi_p)\mathcal{O}_K \cap \mathcal{O}_K$ e $\alpha = a\theta + b\sigma(\theta) + c\sigma^2(\theta) \in \mathcal{O}_K$. Então $\alpha \in \mathfrak{p}_K$ se, e somente se, $a + b + c \in p\mathbb{Z}$. Visto que $N(\mathfrak{p}_K) = p$ e $\mathfrak{D}_K = \pm p^2$, temos

$$\delta(\sigma_K(\mathfrak{p}_K)) = \frac{(\frac{\sqrt{2p}}{2})^3}{p^2} = \frac{1}{2\sqrt{2p}}.$$

Quando $p = 7$, temos

$$\delta(\sigma(\mathfrak{p}_K)) = \frac{(\frac{\sqrt{2 \cdot 7}}{2})^3}{7^2} = \frac{1}{2\sqrt{14}} \approx 0,1336.$$

3.5 Outros Reticulados de Posto 3

Nesta Seção abordaremos os reticulados de posto 3 em $\mathbb{R}^3$, obtidos via representação geométrica de $\mathbb{Z}$ -módulos de anéis de inteiros algébricos; imitando, sob um certo ponto de vista, o Método de Minkowski para ideais ordinários.

Este procedimento generaliza o Método de Minkowski e portanto, em princípio, capaz de gerar resultados mais abrangentes.

Aparentemente este fato será ilustrado a seguir, isto é, não se conhece, até a presente data, a representação geométrica de um ideal em algum corpo de números de grau 3 cuja densidade de centro coincida com a de Λ_3 ; entretanto exibiremos um reticulado de posto 3, com a mesma densidade de centro de Λ_3 , no entanto obtido a partir de um $\mathbb{Z}$ -módulo contido em uma cúbica.

Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e α, β, γ as raízes de f . Para que α, β, γ sejam reais é necessário e suficiente que a derivada de f se anule em dois pontos distintos, digamos x_1 e x_2 , e que $f(x_1)$ e $f(x_2)$ tenham sinais distintos, isto é, $f(x_2) < 0 < f(x_1)$, admitindo, sem perda de generalidade, que $x_1 < x_2$.

Este comentário é resumido formalmente no seguinte resultado:

Lema 3.2 [5] *Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e α, β, γ as raízes de f . Para que α, β, γ sejam reais é necessário e suficiente que*

$$a^2 - 3b > 0 \text{ e que } (\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|.$$

Demonstração. Sendo $f(X) = X^3 + aX^2 + bX + c$, a sua derivada é $f'(X) = 3X^2 + 2aX + b$, cujas raízes são:

$$x_1 = \frac{-a - \sqrt{a^2 - 3b}}{3} \text{ e } x_2 = \frac{-a + \sqrt{a^2 - 3b}}{3}.$$

Daí, a necessidade de $a^2 - 3b$ ser um número positivo. Agora

$$\begin{aligned} f(x_1) &= \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right)^3 + a \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right)^2 + b \left(\frac{-a - \sqrt{a^2 - 3b}}{3} \right) + c \\ &= \frac{1}{27} (2a^3 + 2a^2 \sqrt{a^2 - 3b} - 9ab - 6b \sqrt{a^2 - 3b} + 27c) \\ &= \frac{1}{27} (2a^3 + 2(a^2 - 3b) \sqrt{a^2 - 3b} - 9ab + 27c) \end{aligned}$$

e, portanto, $f(x_1) > 0$ se, e somente se $(\sqrt{a^2 - 3b})^3 > \frac{-2a^3 + 9ab - 27c}{2}$.

Analogamente,

$$\begin{aligned} f(x_2) &= \left(\frac{-a + \sqrt{a^2 - 3b}}{3} \right)^3 + a \left(\frac{-a + \sqrt{a^2 - 3b}}{3} \right)^2 + b \left(\frac{-a + \sqrt{a^2 - 3b}}{3} \right) + c \\ &= \frac{1}{27} (2a^3 - 2a^2 \sqrt{a^2 - 3b} - 9ab + 6b \sqrt{a^2 - 3b} + 27c) \\ &= \frac{1}{27} (2a^3 - 2(a^2 - 3b) \sqrt{a^2 - 3b} - 9ab + 27c) \end{aligned}$$

e, portanto, $f(x_2) < 0$ se, e somente se $(\sqrt{a^2 - 3b})^3 > -\frac{-2a^3 + 9ab - 27c}{2}$. Tendo em vista que a recíproca é imediata isto completa a demonstração do Lema.

□

Considerando a desigualdade $(\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|$ do Lema 3.2, podemos elevar ambos os membros ao quadrado e obtemos uma outra desigualdade, a saber:

Corolário 3.1 [5] *Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e α, β, γ as raízes de f . Para que α, β, γ sejam reais é necessário e suficiente que*

$$a^2 - 3b > 0 \text{ e } c(27c + 4a^3 - 18ab) < b^2(a^2 - 4b).$$

Das relações de Girard, sendo α, β, γ as raízes de

$$f(X) = X^3 + aX^2 + bX + c,$$

podemos deduzir que:

$$\begin{cases} \alpha + \beta + \gamma = -a \\ \alpha\beta + \alpha\gamma + \beta\gamma = b \\ \alpha\beta\gamma = -c \end{cases}$$

Sejam $f(X) = X^3 + aX^2 + bX + c$; $a, b, c \in \mathbb{Z}$ e α, β, γ as raízes de f .

Supondo

$$(\sqrt{a^2 - 3b})^3 > \left| \frac{2a^3 - 9ab + 27c}{2} \right|,$$

sejam

$$\begin{cases} v_1 = (\alpha, \beta, \gamma), \\ v_2 = (\gamma, \alpha, \beta), \\ v_3 = (\beta, \gamma, \alpha) \end{cases}$$

três vetores de $\mathbb{R}^3$ e Λ o reticulado de $\mathbb{R}^3$ gerado pelos vetores v_1, v_2, v_3 . A densidade de centro de Λ é dada por

$$\frac{\rho^3}{|\det T|},$$

sendo T a matriz de ordem 3 cujas entradas são as coordenadas dos vetores v_1, v_2 e v_3 , ou seja,

$$T = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{pmatrix}$$

e ρ é o raio de empacotamento de Λ , isto é,

$$\rho = \frac{1}{2} \cdot \min\{|v|; v \in \Lambda, v \neq 0\}.$$

Lema 3.3 [5] *O determinante da matriz T vale $-a(a^2 - 3b)$.*

Demonstração. Podemos ver que $\det T = \alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma$. Por outro lado, sendo

$$\alpha + \beta + \gamma = -a, \text{ segue que}$$

$$\alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma) = a^2, \text{ ou seja,}$$

$$\alpha^2 + \beta^2 + \gamma^2 = a^2 - 2b. \quad (3.4)$$

Multiplicando o lado esquerdo da Equação 3.4, por $\alpha + \beta + \gamma$ e o lado direito por $-a$ obtemos a equação

$$\begin{aligned} & \alpha^3 + \beta^3 + \gamma^3 + \alpha\beta^2 + \alpha\gamma^2 + \beta\alpha^2 + \beta\gamma^2 + \gamma\alpha^2 + \gamma\beta^2 \\ &= \alpha^3 + \beta^3 + \gamma^3 + \alpha(\alpha + \beta) + \alpha\gamma(\alpha + \gamma) + \beta\gamma(\beta + \gamma) \\ &= \alpha^3 + \beta^3 + \gamma^3 - \alpha\beta(\gamma + a) - \alpha\gamma(\beta + a) + \beta\gamma(\alpha + a) \\ &= -a(a^2 - 2b). \text{ Mas,} \end{aligned}$$

$$\alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma - a(\alpha\beta + \alpha\gamma + \beta\gamma) = -a^3 + 2ab$$

e, conseqüentemente,

$$\alpha^3 + \beta^3 + \gamma^3 - 3\alpha\beta\gamma = -a^3 + 3ab.$$

Portanto $\det T = -a^3 + 3ab$. □

Lema 3.4 [5] *Seja $v = Xv_1 + Yv_2 + Zv_3$ um vetor de Λ então*

$$|v|^2 = (a^2 - 2b)(X^2 + Y^2 + Z^2) + 2b(XY + XZ + YZ).$$

Demonstração. Segue do fato de que

$$v = (\alpha X + \beta Y + \gamma Z, \gamma X + \alpha Y + \beta Z, \beta X + \gamma Y + \alpha Z)$$

e das relações obtidas anteriormente □

Conhecendo o valor de $\det T$ e a expressão da forma quadrática $Q(X, Y, Z)$ que mede o quadrado do comprimento do vetor $v = Xv_1 + Yv_2 + Zv_3$ de Λ , ao minimizarmos a forma quadrática com entradas inteiras não todas nulas, podemos determinar o raio de empacotamento e, conseqüentemente, a densidade de centro de Λ .

Exemplo 3.11 Seja $f(X) = (X-1)(X-2)(X-3) = X^3 - 6X^2 + 11X - 6$. Claramente, $f(X)$ satisfaz as condições do Lema 3.2, e

$$Q(X, Y, Z) = 14(X^2 + Y^2 + Z^2) + 22(XY + XZ + YZ)$$

é a forma quadrática que mede o quadrado do comprimento dos vetores de Λ e seu menor valor é atingido em 6 para a entrada $(1, -1, 0)$. Assim sendo, o raio de empacotamento é $\rho = \frac{\sqrt{6}}{2}$ e a densidade de centro de Λ vale

$$\delta(\Lambda) = \frac{(\sqrt{6}/2)^3}{18} = \frac{\sqrt{6}}{24} \approx 0,1021.$$

Exemplo 3.12 Seja $f(X) = X^3 + 6X^2 + 9X + 1$. É fácil ver que $f(X)$ satisfaz as condições do Lema 3.2. A forma quadrática

$$Q(X, Y, Z) = 18(X^2 + Y^2 + Z^2 + XY + XZ + YZ)$$

atinge o valor mínimo 18 ($X = 1, Y = Z = 0$). Logo $\rho = \frac{\sqrt{18}}{2}$ e

$$\delta(\Lambda) = \frac{(\sqrt{18}/2)^3}{54} = \frac{1}{4\sqrt{2}} \approx 0,1768.$$

O reticulado do exemplo acima tem a mesma densidade de centro de Λ_3 , que é o mais denso reticulado nessa dimensão.



Referências Bibliográficas

- [1] Flores, A. L. "*Representação Geométrica de Ideais de Corpos de Números.*" Dissertação de Mestrado, IMECC - UNICAMP, 1996.
- [2] Flores, A.L. "*Reticulados em Corpos Abelianos.*" Tese de Doutorado, FEEC - UNICAMP, 2000.
- [3] Herstein, I. N., "*Tópicos de Álgebra.*" Editora Polígono S.A. 1970.
- [4] Monteiro, L. H. J.: "*Teoria de Galois.*" Publicações do Instituto de Pesquisas Matemáticas da Universidade de São Paulo.1969.
- [5] Nóbrega, T. P., "Cúbicas Reais, Algumas Aplicações." *Anais do VI Encontro de Álgebra USP* - UNICAMP, 1997.
- [6] Stewart, I. N. and Tall, D. O., "*Algebraic Number Theory.*" Chapman and Hall, 1986.
- [7] Samuel, P., "*Algebraic Number Theory.*" Hermann, 1970.
- [8] Washington, L.C., "*Introduction to Cyclotomic Fields.*" Spring-Verlag, 1982.



