Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Uma Prova Alternativa do Teorema de Cohn em Soma de Quatro Quadrados

por

Elaynne Xavier Souza Araújo

sob orientação do

Prof. Dr. Orlando Stanley Juriaans

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Março/2006

João Pessoa - PB

Uma Prova Alternativa do Teorema de Cohn em Soma de Quatro Quadrados

por

Elaynne Xavier Souza Araújo

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Orlando Stanley Juriaans - IME-USP (Orientador)

Prof. Dr. Roberto Callejas Bedregal - UFPB

Prof. Dr. João Montenegro de Miranda - UECE

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Março/2006

Agradecimentos

- A Deus, por tudo, pois sem Ele nada seria possível.

- Ao Prof. Dr. *Antônio de Andrade e Silva*, pela paciência, pelo incentivo, pela amizade e principalmente pela contribuição direta na realização deste trabalho.

- Ao Prof. Dr. *Orlando Stanley Juriaans*, pela confiança e colaboração na realização deste.

- A minha mãe, ao meu pai e aos meus irmãos, pelo apoio total.

- A todos os colegas do curso de mestrado, pelo incentivo e amizade. E em especial aos amigos e companheiros: Elisandra de Fátima Gloss de Moraes e Reinaldo de Marchi.

- A amiga Josefa Mônica Almeida Silva, pelo companheirismo.

- Ao Aldinei Peres da Silva, pelo incentivo.

- Aos professores do Departamento de Matemática - UFMT - Campus de Rondonópolis.

- Aos professores da Pós-Graduação, pelo conhecimento e experiência transmitidos.

- Ao CNPq pelo suporte financeiro.

Dedicatória

À minha querida família.

Resumo

Mostraremos, através da combinação da geometria de números de Minkowski com o anel de quatérnios Cubianos, que todo inteiro algébrico totalmente positivo em $\mathbb{Z}[\sqrt{2}]$ com coeficiente par no termo radical é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$.

Abstract

We will show, through the combination of geometry of numbers of Minkowski with the ring of quaternion Cubianos, that all totally positive algebraic integer in $\mathbb{Z}[\sqrt{2}]$ with even coefficient on the radical term is the sum of four squares from $\mathbb{Z}[\sqrt{2}]$.

Notação

R - Anel

$R[x]$ - Anel dos polinômios sobre R

$U(R)$ - Conjunto das unidades de R

$\mathcal{O}_d$ - Anel dos inteiros

$\mathbb{Z}_K$ - Anel dos inteiros de K

$\mathbb{Z}_p$ - Anel dos inteiros módulo p

$\mathbb{Z}$ - Conjunto dos números inteiros

$\mathbb{Q}$ - Conjunto dos números racionais

$\mathbb{Q}(\sqrt{d})$ - Corpo quadrático

$\mathbb{R}$ - Conjunto dos números reais

$\mathbb{C}$ - Conjunto dos números complexos

$\mathbb{H}$ - Anel de quatérnios

$\mathbb{Z}_H$ - Anel de quatérnios de Hurwitz

$\mathbb{Z}_C$ - Anel de quatérnios Cubianos

$\langle x \rangle$ - Ideal principal gerado por x

$\langle a_1, a_2, \ldots, a_n \rangle$ - ideal gerado por $\{a_1, a_2, \ldots, a_n\}$

$\mathrm{Ann}_R(X)$ - Anulador de X em R

$\mathrm{mdc}(a, b)$ - Máximo divisor comum de a e b

$\frac{R}{I}$ - Anel quociente de R sobre I

F/K - Extensão de um corpo F sobre um corpo K

B_ρ - bola de raio ρ centrado na origem

p_π - Polinômio característico de π

$\equiv$ - Congruente

$|$ - Divide

$\simeq$ - Isomorfo

$\forall$ - Para qualquer

$\sum$ - Soma

$\prod$ - Produto

$\det \mathbf{A}$ - determinante da matriz $\mathbf{A}$

$\lfloor x \rfloor$ - menor inteiro menor do que ou igual a x

$\mathrm{tr}(\alpha)$ - Traço de α

$N(\alpha)$ - Norma de α

$K(\alpha_1, \ldots, \alpha_n)$ - menor subcorpo contendo $\alpha_1, \ldots, \alpha_n$ e K

$\Delta[\alpha_1, \ldots, \alpha_n]$ - discriminante de $\{\alpha_1, \ldots, \alpha_n\}$

Sumário

Introdução

O problema de escrever um inteiro positivo como soma de quadrados foi objeto de estudo de vários matemáticos como Fermat, Lagrange, Minkowski, Hurwitz.

Uma demonstração de que todo inteiro positivo é soma de quatro quadrados foi dada por Fermat, em 1636, mas a primeira demonstração publicada foi dada por Lagrange, em 1770.

Várias técnicas foram usadas para demonstrar o teorema clássico dos quatro quadrados para inteiros positivos. Hurwitz usou o seu anel de quatérnios, já Minkowski estudou o problema sob um ponto de vista mais geométrico, usando para isso a sua geometria de números.

Para a representação de somas de quatro quadrados de inteiros em corpos quadráticos, foram utilizados o método da formas modulares de duas variáveis. Em 1928, Götzky usando formas modulares, representou um inteiro totalmente positivo em $\mathbb{Q}(\sqrt{5})$ como soma de quatro quadrados. E, em 1960, Cohn, usando a mesma técnica, mostrou que todo inteiro totalmente positivo em $\mathbb{Q}(\sqrt{2})$ ou em $\mathbb{Q}(\sqrt{3})$ pode ser escrito como soma de quatro quadrados.

Uma prova alternativa do teorema de Cohn, através da combinação da geometria de números de Minkowski com o anel de quatérnios Cubianos, mostra que todo inteiro totalmente positivo em $\mathbb{Q}(\sqrt{2})$ com coeficiente par no termo radical é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$.

No primeiro capítulo apresentaremos alguns resultados de corpos quadráticos que serão usados nos capítulos seguintes. No segundo capítulo introduziremos o anel de quatérnios $\mathbb{H}$, onde os elementos se apresentam da seguinte forma

$$\alpha = z_1 + z_2 j \text{ onde } z_1, z_2, \in \mathbb{C},$$

e o anel de quatérnios de Hurwitz que é o $\mathbb{Z}$-módulo

$$\mathbb{Z}_H = \left\{ x_0 + x_1 i + x_2 j + x_3 k : \text{ ou } x_i \in \mathbb{Z}, \forall i \text{ ou } x_i \in \mathbb{Z} + \frac{1}{2}, \forall i \right\}$$

e suas respectivas propriedades. Também apresentaremos o teorema clássico da soma de quatro quadrados sob as perspectivas de Lagrange e de Hurwitz. No terceiro capítulo introduziremos o anel de quatérnios Cubianos $\mathbb{Z}_C$ que é o $\mathbb{Z}[\sqrt{2}]$-módulo

$$\mathbb{Z}_C = \mathbb{Z}[\sqrt{2}][1, \rho_1, \rho_2, \rho_3],$$

onde

$$\rho_1 = \frac{\sqrt{2}}{2}(1+i), \ \ \rho_2 = \frac{\sqrt{2}}{2}(1+j) \ \text{ e } \ \rho_3 = \rho = \frac{1}{2}(1+i+j+k),$$

e suas propriedades. E mostraremos, que

$$\pi = a + 2b\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$

um inteiro algébrico totalmente positivo é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$, através da combinação da geometria de números de Minkowski com o anel de quaténios Cubianos. E no quarto capítulo, que colocamos como apêndice, apresentaremos algumas definições e resultados da teoria de módulos, bem como, alguns resultados de extensões de corpos, de traços e normas, de inteiros algébricos e de reticulados.

Capítulo 1

Corpos Quadráticos

Neste capítulo caracterizaremos os corpos quadráticos $\mathbb{Q}[\sqrt{d}]$, onde d é um inteiro livre de quadrados, juntamente com suas propriedades, que serão necessários para os capítulos subseqüentes. Para maiores detalhes vide [2, 11].

Um *corpo quadrático* é um subcorpo F de $\mathbb{C}$ de dimensão 2 sobre $\mathbb{Q}$, ou seja, $[F, \mathbb{Q}] = 2$. Cada $\alpha \in F = \mathbb{Q}(\sqrt{d})$ será raiz de um polinômio

$$f = \text{irr}(\alpha, \mathbb{Q}) = x^2 + ax + b, \text{ com } a, b \in \mathbb{Z}.$$

Assim,

$$\alpha = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \text{ ou } 2\alpha = -a \pm \sqrt{a^2 - 4b}.$$

Seja $a^2 - 4b = c^2 d$, onde $c, d \in \mathbb{Z}$ e d livre de quadrado. Então

$$F = \mathbb{Q}(\alpha) = \mathbb{Q}(2\alpha) = \mathbb{Q}(-a \pm c\sqrt{d}) = \mathbb{Q}(\sqrt{d}).$$

Se d é positivo, F é chamado um *corpo quadrático real* e se d é negativo, F é chamado um *corpo quadrático imaginário*.

Seja F qualquer corpo quadrático. Então

$$\mathbb{Z}_F = F \cap \overline{\mathbb{Z}}$$

é chamado o *anel dos inteiros* de F, onde

$$\overline{\mathbb{Z}} = \{\alpha \in \mathbb{C} : \alpha \text{ é um inteiro algébrico}\} = \mathbb{Z}_{\mathbb{C}}.$$

Pela Proposição A.26, se $\alpha \in F$, então existe $a \in \mathbb{Z}$ tal que $a\alpha \in \mathbb{Z}_F$. Além disso, se $\alpha \in \mathbb{Z}_F$, então $\text{tr}(\alpha), N(\alpha) \in \mathbb{Z}$ e $F = \mathbb{Q}[\alpha]$, para algum $\alpha \in \overline{\mathbb{Z}}$.

Uma $\mathbb{Q}$-base de F

$$\{\alpha_1, \ldots, \alpha_n\}$$

é chamada *base integral* para $\mathbb{Z}_F$ se $\alpha_i \in \mathbb{Z}_F$, $i = 1, \ldots, n$, e todo $\alpha \in \mathbb{Z}_F$ pode ser escrito de modo único na forma

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

onde $a_i \in \mathbb{Z}$.

Teorema 1.1 *Sejam F um corpo quadrático e $\mathbb{Z}_F$ o seu anel de inteiros. Então existe uma $\mathbb{Q}$-base*

$$\{\alpha_1, \ldots, \alpha_n\}$$

para F, a qual é uma $\mathbb{Z}$-base para $\mathbb{Z}_F$, e $(\mathbb{Z}_F, +)$ é um grupo abeliano livre de posto n.

Prova. Temos que $\mathbb{Z}_F$ está contido em um $\mathbb{Z}$-módulo finitamente gerado. Assim, $\mathbb{Z}_F$ é um $\mathbb{Z}$-módulo finitamente gerado. Logo, existem elementos $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_F$ tais que

$$\mathbb{Z}_F = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_m.$$

Assim, $\mathbb{Z}_F$ é um grupo abeliano livre. É claro que

$$\{\alpha_1, \ldots, \alpha_m\}$$

é um conjunto linearmente independente sobre $\mathbb{Q}$. Como $\mathbb{Z}^{-1}\mathbb{Z}_F = F$, logo

$$\{\alpha_1, \ldots, \alpha_n\}$$

é uma $\mathbb{Q}$-base para F. ■

Teorema 1.2 *Se $d \equiv 2$ ou $3 \pmod 4$, então $B = \{1, \sqrt{d}\}$ é uma base integral de $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$. Se $d \equiv 1 \pmod 4$, então $B = \{1, \eta\}$, onde $\eta = \frac{1+\sqrt{d}}{2}$, é uma base integral de $\mathcal{O}_d = \mathbb{Z}[\eta]$.*

Prova. Se $d \equiv 2$ ou $3 (\mathrm{mod}\, 4)$, então $\mathcal{O}_d = \mathbb{Z}[\sqrt{d}]$ e $\alpha \in \mathcal{O}_d$ é da forma $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, e $\mathrm{irr}(\sqrt{d}, \mathbb{Q}) = x^2 - d$ temos que

$$\begin{aligned} \phi_\alpha(1) &= \alpha \\ \phi_\alpha(\sqrt{d}) &= bd + a\sqrt{d}. \end{aligned}$$

Logo, $\mathcal{O}_d$ é isomorfo ao conjunto das matrizes da forma

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \text{ onde } a, b \in \mathbb{Z}.$$

Neste caso,

$$Tr(\alpha) = 2a \text{ e } N(\alpha) = a^2 - db^2.$$

Assim, o discriminante associado à base B é dado por

$$D(B) = \det \begin{pmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Como $Tr(\alpha)$ é um número inteiro par temos que o discriminante de qualquer base inteira B' de $\mathcal{O}_d$ é um múltiplo de 4, por exemplo $D(B') = 4m$. Assim, se r é o determinante da matriz mudança de base, então $D(B) = r^2 D(B')$ ou $d = r^2 m$. Suponhamos que $|m| < |d|$. Então

$$|m| < \left|r^2 m\right| \Rightarrow |r| > 1.$$

Logo, d possui um fator quadrático, o que é uma contradição. Portanto, a base $B = \{1, \sqrt{d}\}$ é integral.

Agora, se $d \equiv 1 \pmod 4$, então $\mathcal{O}_d = \mathbb{Z}[\eta]$ cada $\alpha \in \mathcal{O}_d$ é da forma $\alpha = a + b\eta$, com $a, b \in \mathbb{Z}$, e $\text{irr}(\eta, \mathbb{Q}) = x^2 - x + \frac{1-d}{4}$ temos que

$$\begin{aligned} \phi_\alpha(1) &= \alpha \\ \phi_\alpha(\eta) &= \frac{b(d-1)}{4} + (a+b)\eta \end{aligned}$$

Logo, $\mathcal{O}_d$ é isomorfo ao conjunto das matrizes da forma

$$\begin{pmatrix} a & \frac{b(d-1)}{4} \\ b & a+b \end{pmatrix}, \text{ onde } a, b \in \mathbb{Z}.$$

Neste caso,

$$Tr(\alpha) = 2a + b \text{ onde } N(\alpha) = a^2 + ab - \frac{b^2(d-1)}{4}.$$

Assim, o discriminante associado à base B é dado por

$$D(B) = \det \begin{pmatrix} Tr(1) & Tr(\eta) \\ Tr(\eta) & Tr(\eta^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} = d.$$

Como $Tr(\alpha)$ é um número inteiro temos que o discriminante de qualquer base inteira B' de $\mathcal{O}_d$ é um inteiro, por exemplo $D(B') = m$. Assim, se r é o determinante da matriz

mudança de base, então $d = r^2 m$. Suponhamos que $|m| < |d|$. Então $|r| > 1$. Logo, d possui um fator quadrático, o que é uma contradição. Portanto, a base $B = \{1, \eta\}$ é integral. ■

Lema 1.3 *Seja $d \in \mathbb{N} - \{1\}$ livre de quadrados. Então*:

1. *Para cada $n \in \mathbb{N}$ existem $x, y \in \mathbb{N}$ tais que*

$$0 < \left| x - y\sqrt{d} \right| < \frac{1}{n} \leq \frac{1}{y}.$$

2. *Existe um número infintito de pares $(x, y) \in \mathbb{N} \times \mathbb{N}$ tais que*

$$0 < \left| x - y\sqrt{d} \right| < \frac{1}{y} \ \ e \ \ 0 < \left| x^2 - dy^2 \right| < 1 + 2\sqrt{d}.$$

3. *A equação de Pell $x^2 - dy^2 = 1$ tem uma solução não-nula $(x, y) \in \mathbb{N} \times \mathbb{N}$ com $(x, y) \neq (1, 0)$.*

Prova. 1. Para cada $x \in \mathbb{R}$, temos que

$$x - \lfloor x \rfloor \in [0, 1). \text{ onde } \ \lfloor x \rfloor = \max \{n \in \mathbb{Z} : n \leq x\}$$

Assim, os números reais

$$0, \sqrt{d} - \lfloor \sqrt{d} \rfloor, \ldots, n\sqrt{d} - \lfloor n\sqrt{d} \rfloor \tag{1.1}$$

pertencem ao intervalo $[0, 1)$. Agora, consideremos a partição de $[0, 1)$ sob a forma

$$[0, 1) = \bigcup_{k=0}^{n-1} \left[\frac{k}{n}, \frac{k+1}{n} \right). \tag{1.2}$$

É claro que, pelo menos, dois dos reais em (1.1) estejam em um mesmo intervalo em (1.2), digamos

$$k_1\sqrt{d} - \lfloor k_1\sqrt{d} \rfloor \ \text{ e } \ k_2\sqrt{d} - \lfloor k_2\sqrt{d} \rfloor, \ \text{ com } \ k_1 < k_2.$$

Então

$$\left| (k_2 - k_1)\sqrt{d} - \left(\lfloor k_2\sqrt{d} \rfloor - \lfloor k_1\sqrt{d} \rfloor \right) \right| < \frac{1}{n}$$

Assim, existem

$$x = \lfloor k_2\sqrt{d} \rfloor - \lfloor k_1\sqrt{d} \rfloor, \ \ y = k_2 - k_1 \in \mathbb{N}$$

tais que

$$\left|x - y\sqrt{d}\right| < \frac{1}{n}, \text{ pois } d \geq 2.$$

Como $0 < y = k_2 - k_1 \leq k_2 \leq n$ temos que

$$\frac{1}{n} \leq \frac{1}{y}.$$

Portanto,

$$\left|x - y\sqrt{d}\right| < \frac{1}{n} \leq \frac{1}{y}.$$

2. Suponhamos, por absurdo, que existe um número finito de pares

$$(x_1, y_1), \ldots, (x_k, y_k) \in \mathbb{N} \times \mathbb{N}$$

tais que

$$\left|x_j - y_j\sqrt{d}\right| < \frac{1}{y_j} \text{ e } \left|x^2 - dy^2\right| < 1 + 2\sqrt{d}, j = 1, ..., k.$$

Tomando

$$\delta = \min\left\{\left|x_j - y_j\sqrt{d}\right|, \ j = 1, ..., k\right\} \in \mathbb{R},$$

temos que existe $m \in \mathbb{N}$ tal que $0 < \frac{1}{m} < \delta$, pois $\mathbb{R}$ é Arquimediano. Pelo item 1., existem $x, y \in \mathbb{N}$ tais que

$$\left|x - y\sqrt{d}\right| < \frac{1}{m} \leq \frac{1}{y} \text{ e } \left|x^2 - dy^2\right| < 1 + 2\sqrt{d},$$

pois

$$\left|x^2 - dy^2\right| = \left|x - y\sqrt{d}\right|\left|x + y\sqrt{d}\right| \text{ e } \left|x + y\sqrt{d}\right| \leq \left|x - y\sqrt{d}\right| + \left|2y\sqrt{d}\right| < \frac{1}{y} + 2y\sqrt{d},$$

implica que

$$\left|x^2 - dy^2\right| < \frac{1}{y}\left(\frac{1}{y} + 2y\sqrt{d}\right) = \frac{1}{y^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Como $\frac{1}{m} < \delta$ temos que $(x, y) \neq (x_j, y_j), \ j = 1, \ldots, k$, o que é uma contradição.

3. Pelo item 2. existe pelo menos um $r \in \mathbb{R}$ (dependendo de d) que corresponde a um número infinito de pares $(x, y) \in \mathbb{N} \times \mathbb{N}$ tais que

$$\left|x^2 - dy^2\right| = r, \text{ com } 0 < r < 1 + 2\sqrt{d}.$$

Assim, para pelo menos um dos números $\varepsilon \in \{-1, 1\}$ existe um número infinito de pares $(x, y) \in \mathbb{N} \times \mathbb{N}$ tais que

$$x^2 - dy^2 = \varepsilon r.$$

Como existem somente r^2 restos módulo r:

$$x \equiv 0, 1, \ldots, (r-1) \pmod{r} \text{ e } y \equiv 0, 1, \ldots, (r-1) \pmod{r},$$

temos que existem duas soluções diferentes $(x_1, y_1), (x_2, y_2) \in \mathbb{N} \times \mathbb{N}$ tais que

$$x_1 \equiv x_2 \pmod{r} \text{ e } y_1 \equiv y_2 \pmod{r}.$$

Então

$$\alpha = \frac{x_1 x_2 - d y_1 y_2}{r}, \beta = \frac{x_2 y_1 - x_1 y_2}{r} \in \mathbb{Z}$$

satisfaz

$$\left(x_1 + y_1\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right) = r\left(\alpha + \beta\sqrt{d}\right) \tag{1.3}$$

Tomando a cojungação na equação (1.3), temos que

$$\left(x_1 - y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right) = r\left(\alpha - \beta\sqrt{d}\right) \tag{1.4}$$

Multiplicando membro a membro as equações (1.3) e (1.4), temos que

$$r^2\left(\alpha^2 - d\beta^2\right) = \left(x_1^2 - d y_1^2\right)\left(x_2^2 - d y_2^2\right) = (\varepsilon r)(\varepsilon r) = r^2.$$

Assim,

$$\alpha^2 - d\beta^2 = 1.$$

Portanto, o par $(|\alpha|, |\beta|) \in \mathbb{N} \times \mathbb{N}$ é uma solução da equação de Pell.

Afirmação. $\beta \neq 0$.

De fato, se $\beta = 0$, então

$$\frac{x_1}{x_2} = \frac{y_1}{y_2} = \kappa > 0,$$

de modo que

$$\varepsilon r = x_1^2 - d y_1^2 = \kappa^2\left(x_2^2 - d y_2^2\right) = \kappa^2 \varepsilon r \Rightarrow \kappa^2 = 1 \Rightarrow \kappa = 1.$$

Logo, $(x_1, y_1) = (x_1, y_1)$, o que é uma contradição. ■

Corolário 1.4 *Sejam $(x_1, y_1), (x_2, y_2) \in \mathbb{N} \times \mathbb{N}$ soluções da equação de Pell, x_3 e y_3 são determinados por*

$$\begin{aligned} \pm\left(x_1 + y_1\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right) &= x_3 + y_3\sqrt{d} \text{ e} \\ \pm\left(x_1 + y_1\sqrt{d}\right)\left(\frac{1}{x_2 + y_2\sqrt{d}}\right) &= x_4 + y_4\sqrt{d}. \end{aligned}$$

Então (x_3, y_3) e (x_4, y_4) são, também, soluções.

Teorema 1.5 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathcal{O}_d$ o anel dos inteiros de K.*

1. *$\alpha \in U(\mathcal{O}_d)$ se, e somente se, $N(\alpha) = \pm 1$.*
2. *Se $N(\alpha) = p$, onde p é um número primo, então α é um elemento irredutível de $\mathcal{O}_d$.*
3. *Se $d = -1$, então $U(\mathcal{O}_d) = \{\pm 1, \pm i\}$, onde $i^2 = -1$.*
4. *Se $d = -3$, então $U(\mathcal{O}_d) = \{\pm 1, \pm\omega, \pm\omega^2\}$, onde $\omega = \exp(\frac{2\pi i}{3})$.*
5. *Se $d < 0$ e $d \notin \{-3, -1\}$, então $U(\mathcal{O}_d) = \{-1, 1\}$.*
6. *Se $d > 0$, então $U(\mathcal{O}_d) = \{\pm\omega^n : n \in \mathbb{Z}\}$, onde ω é a unidade fundamental de $\mathcal{O}_d$ maior do que 1.*

Prova. 1. e 2. segue da Proposição A.26.

3. Se $d = -1$, então $\mathcal{O}_d = \mathbb{Z}[i]$. Dado $\alpha \in U(\mathcal{O}_d)$ existe $\beta \in \mathcal{O}_d$ tal que $\alpha\beta = 1$. Logo,

$$N(\alpha)\, N(\beta) = N(1) = 1.$$

Tomando $\alpha = a + ib$ e $\beta = c + id$, obtemos

$$(a^2 + b^2)(c^2 + d^2) = 1.$$

Logo, $a^2 + b^2 = 1$. Neste caso, as únicas soluções inteiras são $(\pm 1, 0)$ e $(0, \pm 1)$. Portanto, $U(\mathcal{O}_d) = \{\pm 1, \pm i\}$.

4. Se $d = -3$, então $\mathcal{O}_d = \mathbb{Z}[\omega]$, onde $\omega = \frac{-1+\sqrt{3}i}{2}$. Dado $\alpha \in U(\mathcal{O}_d)$, existe $\beta \in \mathcal{O}_d$ tal que $\alpha\beta = 1$. Logo,

$$N(\alpha)\, N(\beta) = N(1) = 1.$$

Tomando

$$\alpha = a + b\omega \text{ e } \beta = c + d\omega,$$

obtemos

$$\left(a^2 - ab + b^2\right)\left(c^2 - cd + d^2\right) = 1.$$

Como $N(\alpha) = a^2 - ab + b^2 = 1$ temos que

$$\begin{aligned} 1 &= a^2 - ab + b^2 \\ &= \frac{4a^2 - 2(2a)b + b^2 + 3b^2}{4} \\ &= \frac{(2a - b)^2 + 3b^2}{4}, \end{aligned}$$

assim

$$(2a-b)^2+3b^2=4.$$

Temos então as seguintes possibilidades: $(2a-b)^2=1$ e $b^2=1$, então $b=\pm1\Rightarrow a=0$. E $(2a-b)^2=4$ e $b^2=0$, então $b=0\Rightarrow a=\pm1$. Logo, as únicas soluções inteiras são $(\pm1,0)$, $(0,\pm1)$, $(1,-1)$ e $(-1,1)$. Portanto, $U(\mathcal{O}_d)=\{\pm1,\pm\omega,\pm\omega^2\}$.

5. Se $d<-3$, então dado $\alpha\in U(\mathcal{O}_d)$, existe $\beta\in\mathcal{O}_d$ tal que $\alpha\beta=1$. Logo,

$$N(\alpha)\,N(\beta)=N(1)=1.$$

Tomando

$$\alpha=a+b\sqrt{d}\ \text{ e }\ \beta=r+s\sqrt{d},$$

obtemos

$$\left(a^2-db^2\right)\left(r^2-ds^2\right)=1.$$

Logo, $a^2-db^2=1$. Neste caso, as únicas soluções inteiras são $(\pm1,0)$. Finalmente, se $d=-2$, então $a^2+2b^2=1$ e, também, neste caso, as únicas soluções inteiras são $(\pm1,0)$. Portanto, $U(\mathcal{O}_d)=\{-1,1\}$.

6. Se $d>0$. Como a multiplicação por -1 transforma unidade positiva em negativa e a função inversão $x\mapsto\frac{1}{x}$ transforma o conjunto das unidades com $u<1$ no conjunto das unidades com $u>1$ temos que todas as unidades em $U(\mathcal{O}_d)$, além de ±1, são da forma $\pm u$ ou $\pm u^{-1}$, onde u é uma unidade com $u>1$. Pela equação de Pell existe uma unidade $u=x+y\sqrt{d}$ com $x,y\in\mathbb{N}$ e $u>1+\sqrt{d}>1$. Como $\mathbb{N}$ é um conjunto discreto temos que existe uma menor unidade ω com $\omega>1$.

Afirmação. ω^n, com $n\in\mathbb{N}$, são todas as unidades maiores que 1.
De fato, é claro que $\omega^n>1$, para todo $n\in\mathbb{N}$. Seja $z\in U(\mathcal{O}_d)$. Como $z>1$ temos, pela minimalidade de ω, que $z\geq\omega$. Então existe um $m\in\mathbb{N}$ tal que

$$\omega^m\leq z<\omega^{m+1}.$$

Se

$$\omega^m<z<\omega^{m+1},$$

então multiplicando esta inequação por $\omega^{-m}>0$, obtemos

$$1<z\omega^{-m}<\omega.$$

O que contradiz a escolha de ω, pois $z\omega^{-m}\in U(\mathcal{O}_d)$. ■

Lema 1.6 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathcal{O}_d$ o anel dos inteiros de K. Se $\mathcal{O}_d$ é um domínio Euclidiano, então cada elemento primo $\pi \in \mathcal{O}_d$ é divisor de um único número primo $p \in \mathbb{N}$.*

Prova. Sejam π qualquer elemento primo em $\mathcal{O}_d$ e

$$X = \{n \in \mathbb{N} : \pi \text{ divide } n\}.$$

Então $X \neq \emptyset$, pois π divide $|N(\pi)|$. Assim, X contém um menor elemento, digamos k.

Afirmação. k é um número primo.

De fato, se k é composto, digamos $k = k_1k_2$ com $1 < k_1, k_2 < k$, então

$$\pi \mid k_1k_2 \Rightarrow \pi \mid k_1 \text{ ou } \pi \mid k_2,$$

o que contradiz a minimalidade de k. Agora, sejam p e q números primos distintos tais que

$$\pi \mid p \text{ e } \pi \mid q.$$

Então

$$\pi \mid \text{mdc}(p, q) = 1,$$

o que é impossível. ■

Lema 1.7 *$\mathbb{Z}[\sqrt{2}]$ é um domínio euclidiano.*

Prova. É claro que a função $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}_+$ definida por $N(a + b\sqrt{2}) = |a^2 - 2b^2|$ é uma norma em $\mathbb{Z}[\sqrt{2}]$ e $N(\alpha) \leq N(\alpha\beta)$, para todos $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]^*$. Sejam $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$, com $\beta \neq 0$. Se $\alpha = 0$, basta $q = r = 0$. Se $\alpha \neq 0$, então, $\alpha\beta^{-1} = x + y\sqrt{2}$, com $x, y \in \mathbb{Q}$. Podemos escolher $m, n \in \mathbb{Z}$ tais que

$$|x - m| \leq \frac{1}{2} \text{ e } |y - n| \leq \frac{1}{2},$$

Assim,

$$\alpha\beta^{-1} = m + n\sqrt{2} + (x - m) + (y - n)\sqrt{2}.$$

Fazendo $q = m + n\sqrt{2}$ e $r = \beta[(x - m) + (y - n)\sqrt{2}]$, obtemos

$$\alpha = q\beta + r,$$

onde

$$N(r) = N(\beta)\left|(x - m)^2 - 2(y - n)^2\right| \leq N(\beta)\left(\frac{1}{4} + \frac{2}{4}\right) < N(\beta).$$

Portanto, q e r são quociente e resto, respctivamente, na divisão de α por β. ■

Lema 1.8 *2 é um resíduo quadrático de primos da forma* $8n \pm 1$ *e não é um resíduo quadrático de primos da forma* $8n \pm 3$.

Prova. [5, Theorem, 95, p 75]. ■

Lema 1.9 *Sejam* $K = \mathbb{Q}(\sqrt{2})$ *e* $\mathcal{O}_d = \mathbb{Z}[\sqrt{2}]$ *o anel dos inteiros de* K. *Então os elementos primos em* $\mathcal{O}_d$ *são*:

1. $\sqrt{2}$ *e seus associados.*
2. *Os elementos primos da forma* $p = 8n \pm 3$.
3. *Os fatores* $a + b\sqrt{2}$ *de números primos da forma* $p = 8n \pm 1$.

Prova. Sejam $\pi = a + b\sqrt{2}$ qualquer elemento primo em $\mathcal{O}_d$ e p um número primo tal que π divide p. Então existe $\lambda \in \mathcal{O}_d$ tal que

$$p = \pi\lambda \text{ e } N(\pi)N(\lambda) = p^2.$$

Como $N(\pi) \neq 1$ temos que $N(\lambda) = 1$ ou $N(\lambda) = p$. Se $N(\lambda) = 1$, então π é um associado de p. Agora, se $N(\lambda) = p$, então

$$N(\pi) = a^2 - 2b^2 = \pm p. \tag{1.5}$$

1.^{o} **Caso**. Se $p = 2$, então

$$a^2 - 2b^2 = \pm 2 \Rightarrow a^2 = 2b^2 \pm 2.$$

Logo, a^2 é par e, portanto, a é par. Se $a = 2n$, então

$$\pm 2 = a^2 - 2b^2 = (2n)^2 - 2b^2 = 4n^2 - 2b^2 = 2(2n^2 - b^2).$$

Assim,

$$2n^2 - b^2 = \pm 1. \tag{1.6}$$

Portanto,

$$\pi = a + b\sqrt{2} = 2n + b\sqrt{2} = \sqrt{2}(b + n\sqrt{2}).$$

Fazendo $\tau = b + n\sqrt{2}$, obtemos

$$N(\tau) = b^2 - 2n^2 = -(2n^2 - b^2) = \mp 1.$$

Isto implica que existe $\tau \in U(\mathcal{O}_d)$ tal que

$$\pi = \sqrt{2}\tau$$

é um associado de $\sqrt{2}$.

2.^{o} **Caso**. Se $p = 8n \pm 3$, então a equação (1.5) é impossivel, pois estes primos são inertes e além disso 2 não é um resíduo quadrático módulo p, e mais

$$a^2 \equiv 0, 1 \text{ ou } 4 \pmod 8, \forall a \in \mathbb{Z}, \Rightarrow a^2 - 2b^2 \equiv 0, 1, 4, 6 \text{ ou } 7 \pmod 8,$$

ou seja, nunca teremos resto 3 e 5.

3.^{o} **Caso**. Se $p = 8n \pm 1$, então a equação (1.5) tem solução e 2 é um resíduo quadrático módulo p. Assim, p não é um elemento primo em $\mathcal{O}_d$, ou seja, p é decomposto em $\mathcal{O}_d$. Temos que

$$p = \pi\lambda \text{ onde } \pi = a + b\sqrt{2} \text{ e } \lambda = a - b\sqrt{2}.$$

Neste caso, os fatores primos de p em $\mathcal{O}_d$ são:

$$\pi, \pi\omega^n, -\pi, -\pi\omega^n, \lambda, \lambda\omega^n, -\lambda, -\lambda\omega^n,$$

para todo $n \in \mathbb{N}$. ■

Observação 1.10 *Vimos que se p decompõe-se em $\mathcal{O}_d$, então $p = \pi\lambda$, onde $\pi = a + b\sqrt{2}$ e $\lambda = a - b\sqrt{2}$. Portanto,*

$$p = |\pi\overline{\pi}|.$$

Lema 1.11 *Seja $p > 2$ um número primo. Então a equação*

$$x^2 + y^2 + 1 \equiv 0 \pmod p$$

admite uma solução $x_0, y_0 \in \mathbb{Z}$ com

$$0 \leq x_0 \leq \frac{p-1}{2} \text{ e } 0 \leq y_0 \leq \frac{p-1}{2}.$$

Prova. Sejam

$$S_1 = \left\{1 + k^2 : k = 0, 1, \ldots, \frac{p-1}{2}\right\} \text{ e } S_2 = \left\{-l^2 : l = 0, 1, \ldots, \frac{p-1}{2}\right\}.$$

Então, é fácil verificar que quaisquer dois elementos distintos de S_1 (S_2) são incongruentes módulo p. Além disso, como $S_1 \cap S_2 \neq \emptyset$, pois $|\mathbb{Z}_p| = p$, temos que existe um elemento $1 + x_0^2 \in S_1$ que deve ser congruente módulo p com algum elemento $-y_0^2 \in S_2$, isto é,

$$1 + x_0^2 \equiv -y_0^2 \pmod p \text{ com } 0 \leq x_0 \leq \frac{p-1}{2} \text{ e } 0 \leq y_0 \leq \frac{p-1}{2}.$$

■

Lema 1.12 *Seja $p \in \mathbb{N}$ um número primo que se decompõe no anel de inteiros algébricos $\mathcal{O}$ de um corpo quadrático real de discriminante d. Seja π um elemento primo de $\mathcal{O}$ que divide p. Então existem $\kappa, \alpha, \beta, \gamma$ e δ em $\mathcal{O}_d$ tais que*

$$\kappa\pi = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \ \ e \ \ |\kappa\overline{\kappa}| \leq 1,70d.$$

Prova. Como p se decompõe temos que $|\pi\overline{\pi}| = p$. Pelo Lema 1.11, podemos escolher $a, b \in \mathbb{Z}$ tais que

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}.$$

Como $\pi \mid p$ temos que

$$a^2 + b^2 + 1 \equiv 0 \pmod{\pi}.$$

Seja Λ um reticulado em $\mathbb{R}^8$ cuja matriz geradora é

$$M = \begin{bmatrix} 1 & 1 & 0 & 0 & a & a & b & b \\ \varepsilon & \overline{\varepsilon} & 0 & 0 & a\varepsilon & a\overline{\varepsilon} & b\varepsilon & b\overline{\varepsilon} \\ 0 & 0 & 1 & 1 & b & v & -a & -a \\ 0 & 0 & \varepsilon & \overline{\varepsilon} & b\varepsilon & b\overline{\varepsilon} & -a\varepsilon & -a\overline{\varepsilon} \\ 0 & 0 & 0 & 0 & \rho & \overline{\rho} & 0 & 0 \\ 0 & 0 & 0 & 0 & \varepsilon\rho & \overline{\varepsilon\rho} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \rho & \overline{\rho} \\ 0 & 0 & 0 & 0 & 0 & 0 & \varepsilon\rho & \overline{\varepsilon\rho} \end{bmatrix}$$

Assim,

$$d(\Lambda) = \left|(\varepsilon - \overline{\varepsilon})^4 \rho^2 (\overline{\rho})^2\right| \ \text{ ou } \ d^2p^2.$$

E o conjunto dos elementos $(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) \in \mathbb{R}^8$ tais que

$$\sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2} + \sqrt{x_5^2 + x_6^2 + x_7^2 + x_8^2} \leq r$$

é um subconjunto convexo e centrado simetricamente cujo volume, visto no Lema A.33, é $\frac{\pi^4}{280} \cdot r^8$. Agora, escolhendo um r, para aplicarmos o Teorema de Minkowski, obtemos

$$\frac{\pi^4}{280} r^8 \geq 2^8 d^2 p^2 \Rightarrow r^8 \geq \frac{2^8 d^2 280}{\pi^4} p^2 \Rightarrow r = 2,2822 d^{\frac{1}{4}} p^{\frac{1}{4}}.$$

Seja

$$(\alpha, \overline{\alpha}, \beta, \overline{\beta}, a\alpha + b\beta + \mu\rho, a\overline{\alpha} + b\overline{\beta} + \overline{\mu\rho}, b\alpha - a\beta + \nu\rho, b\overline{\alpha} - a\overline{\beta} + \overline{\nu\rho}) = s \neq 0$$

um conjunto do reticulado, onde $\alpha, \beta, \mu, \nu \in \mathcal{O}$. Observemos que

$$\begin{aligned} 0 &\leq (\sqrt[4]{a} - \sqrt[4]{b})^2 = \sqrt{a} - 2\sqrt[4]{ab} + \sqrt{b} \\ 2\sqrt[4]{ab} &\leq \sqrt{a} + \sqrt{b}. \end{aligned}$$

Tomando $a = \kappa\pi$ e $b = \overline{\kappa\pi}$, temos que

$$\begin{aligned} 2\sqrt{\sqrt{\kappa\pi\overline{\kappa\pi}}} &\leq \sqrt{\kappa\pi} + \sqrt{\overline{\kappa\pi}} \\ 2\sqrt{\sqrt{\kappa\pi}\sqrt{\overline{\kappa\pi}}} &\leq \sqrt{\kappa\pi} + \sqrt{\overline{\kappa\pi}}. \end{aligned}$$

Como, $\kappa\pi = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$, onde $\gamma = a\alpha + b\beta + \mu\rho$ e $\delta = b\alpha - a\beta + \nu\rho$, assim

$$\begin{aligned} \alpha^2 + \beta^2 + \gamma^2 + \delta^2 &= \alpha^2 + \beta^2 + (a\alpha + b\beta + \mu\rho)^2 + (b\alpha - a\beta + \nu\rho)^2 \\ &= \alpha^2 + \beta^2 + (a\alpha + b\beta)^2 + \mu^2\rho^2 + (b\alpha - a\beta)^2 + \nu^2\rho^2 \\ &= \alpha^2 + \beta^2 + a^2(\alpha^2 + \beta^2) + b^2(\beta^2 + \alpha^2) + (\gamma^2 + \delta^2) \\ &= (a^2 + b^2 + 1)(\alpha^2 + \beta^2) + (\gamma^2 + \delta^2). \end{aligned}$$

Como

$$a^2 + b^2 + 1 \equiv 0 \pmod{\pi} \Rightarrow \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 \pmod{\pi}.$$

Logo,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \kappa\pi.$$

Temos que $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \kappa\pi$, usando a mesma técnica, encontramos que

$$(\overline{\alpha})^2 + (\overline{\beta})^2 + (\overline{\gamma})^2 + (\overline{\delta})^2 = \overline{\kappa\pi}.$$

Observemos agora que,

$$|s| = \sqrt{a^2} + \sqrt{b^2} = \sqrt{\kappa\pi} + \sqrt{\overline{\kappa\pi}},$$

mas $\sqrt{\kappa\pi} + \sqrt{\overline{\kappa\pi}} < r$, logo,

$$\begin{aligned} 2\sqrt{\sqrt{\kappa\pi}\sqrt{\overline{\kappa\pi}}} &< r = 2,2822 d^{\frac{1}{4}} p^{\frac{1}{4}} \\ 2\sqrt{\sqrt{\kappa\pi\overline{\kappa\pi}}} &< 2,2822 d^{\frac{1}{4}} p^{\frac{1}{4}} \\ 2\sqrt[4]{\kappa\pi\overline{\kappa\pi}} &< 2,2822 d^{\frac{1}{4}} p^{\frac{1}{4}} \\ |\kappa\overline{\kappa}| &< 1,6955 d. \end{aligned}$$

■

Lema 1.13 *Seja $\pi \in \mathcal{O}_2 = \mathbb{Z}[\sqrt{2}]$ elemento primo. Então existem κ,α,β,γ e δ em $\mathcal{O}_2$ tais que*

$$\kappa\pi = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \ \ e \ \ |\kappa\overline{\kappa}| \leq 9.$$

Prova. Se $\pi \in \mathcal{O}_2$ é um elemento primo, então existe um único número $p \in \mathbb{Z}$ tal que π está acima de p. Analisemos três casos:

1.^{o} **Caso**. Se p é inerte, então existe um elemento $\tau \in U(\mathcal{O}_2)$ tal que

$$p = \tau\pi.$$

Consideremos $\kappa = \tau^{-1}$. Assim,

$$\kappa\pi = p = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \ \text{ e } \ |\kappa\overline{\kappa}| = 1.$$

Temos, assim, o caso clássico.

2.^{o} **Caso**. Se p ramifica, então $p = 2$ e existe um elemento $\tau \in U(\mathcal{O}_2)$ tal que

$$\pi = \tau\sqrt{2}.$$

Tomemos $\kappa = \tau^{-1}\sqrt{2}$, logo $|\kappa\overline{\kappa}| = 2$. Então,

$$\kappa\pi = \sqrt{2}\sqrt{2} = 1^2 + 1^2 + 0^2 + 0^2.$$

3.^{o} **Caso**. Se p se decompõe, podemos aplicar o Lema anterior, pois $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ e p se decompõe. Neste caso, $d = 8$. Já que

$$|\kappa\overline{\kappa}| \leq 1,7d = 13,56 \ \text{ e } \ |\kappa\overline{\kappa}| \in \mathbb{Z} \Rightarrow |\kappa\overline{\kappa}| \leq 13.$$

Consideremos um primo $q \in \mathbb{Z}$ inerte em $\mathcal{O}_2$, então é um elemento primo em $\mathcal{O}_2$ tal que $q \mid \kappa\overline{\kappa}$. Logo, $q \mid \kappa$ ou $q \mid \overline{\kappa}$. Como $\overline{q} = q$ segue-se que $q \mid \kappa$ e $q \mid \overline{\kappa}$, logo, $q^2 \mid \kappa\overline{\kappa}$. Mas $\kappa\overline{\kappa} \in \mathbb{Z}$ e $|\kappa\overline{\kappa}| \leq 13$. Vamos observar quando $|\kappa\overline{\kappa}| \in \{10, 11, 12, 13\}$

$$|\kappa\overline{\kappa}| = 13,13 \text{ é inerte, então } 13^2 \mid \kappa\overline{\kappa}, \text{ absurdo .}$$

$$|\kappa\overline{\kappa}| = 12 = 4 \cdot 3,3 \text{ é inerte, e } 4 \text{ é ramificado, não pode ocorrer .}$$

$$|\kappa\overline{\kappa}| = 11,11 \text{ é inerte, então } 11^2 \mid \kappa\overline{\kappa}, \text{ absurdo .}$$

$$|\kappa\overline{\kappa}| = 10, = 2 \cdot 5,2 \text{ é ramificado e } 5, \text{ é inerte, não pode ocorrer .}$$

Portanto, $|\kappa\overline{\kappa}| \leq 9$. ■

Capítulo 2

Teorema Clássico da Soma de Quatro Quadrados

Neste capítulo apresentaremos os dois tipos de quatérnios utilizados na demonstração do teorema clássico dos quatro quadrados, a saber, sobre os números reais e os de Hurwitz, com suas respectivas propriedades. Também mostraremos o teorema clássico sob duas perspectivas, dentre as existentes, que são a de Lagrange e a de Huwirtz, que tratam do teorema utilizando técnicas diferentes.

2.1 Quatérnios

Em um curso de álgebra linear pode ser observado que muitas das propriedades de espaço vetorial são compartilhadas por módulos sobre um anel de divisão. Como um exemplo importante de tal anel de divisão construiremos neste capítulo o anel dos quatérnios.

O anel dos quatérnios sobre os números reais é uma generalização dos números complexos. Na construção do anel de quatérnios, usaremos o corpo dos números complexos $\mathbb{C}$ e o automorfismo de $\mathbb{C}$ sobre $\mathbb{C}$ definido por

$$z \mapsto \overline{z},$$

onde z e $\overline{z} = x - yi$ é o conjugado de $z = x + yi$. Denotaremos por $\mathbb{H} = \mathbb{C}[1, j]$ o espaço vetorial de dimensão 2 sobre $\mathbb{C}$ com $\mathbb{C}$-base $\{1, j\}$ e $j^2 = -1$, sendo j a parte imaginária dos números complexos. Assim, os elementos de $\mathbb{H}$ são escritos de modo único como

$$\alpha = z_1 + z_2 j.$$

Definiremos o produto $\mathbb{H} \times \mathbb{H} \to \mathbb{H}$ por

$$\alpha\beta = (z_1 + z_2 j)\,(w_1 + w_2 j) = (z_1 w_1 - z_2 \overline{w}_2) + (z_1 w_2 + z_2 \overline{w}_1) j.$$

onde $\alpha = z_1 + z_2 j$ e $\beta = w_1 + w_2 j$, onde $z_1, z_2, w_1, w_2 \in \mathbb{C}$. Em particular, o elemento 1 é uma unidade neste produto e os casos especiais deste produto são

$$\alpha 1 = 1\alpha = \alpha, \;\; j^2 = -1, \;\; \text{e} \;\; j\alpha = \overline{\alpha} j.$$

Definimos o *conjugado* de um elemento α em $\mathbb{H}$ por

$$\overline{\alpha} = \overline{(z_1 + z_2 j)} = \overline{z}_1 - z_2 j.$$

A conjugação satisfaz as seguintes propriedades:

1. $\overline{\overline{\alpha}} = \alpha$.
2. $\overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}$.
3. $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$.
4. $\alpha\overline{\alpha} = \overline{\alpha}\alpha$.

A *norma* (reduzida) de um elemento α em $\mathbb{H}$ é definida por

$$N(\alpha) = \alpha\overline{\alpha}.$$

Assim,

$$N(\alpha) = (z_1 + z_2 j)(\overline{z}_1 - z_2 j) = z_1\overline{z}_1 + z_2\overline{z}_2.$$

Como $z\overline{z}$ é um número real positivo para cada $z \in \mathbb{C}$ com $z \neq 0$ temos que $N(\alpha)$ é um número real positivo quando $\alpha \neq 0$. Logo,

$$N(\alpha\beta) = \alpha\beta\overline{(\alpha\beta)} = \alpha\beta\overline{\beta}\,\overline{\alpha} = \alpha N(\beta)\overline{\alpha} = \alpha\overline{\alpha} N(\beta) = N(\alpha)N(\beta).$$

Portanto, $N : \mathbb{H} - \{0\} \to \mathbb{R} - \{0\}$ é um homomorfismo de grupos multiplicativos. Além disso, se $\alpha \in \mathbb{H}$ com $\alpha \neq 0$, então

$$\alpha^{-1} = \frac{1}{N(\alpha)}\overline{\alpha}.$$

Como $\mathbb{C}$ é um espaço vetorial de dimensão 2 sobre $\mathbb{R}$ com $\mathbb{R}$-base $\{1, i\}$ temos que $\mathbb{H}$ é um espaço vetorial de dimensão 4 sobre $\mathbb{R}$ com $\mathbb{R}$-base$\{1, i, j, ij\}$. Fazendo $k = ij$, obtemos

$$\alpha = z_1 + z_2 j = x_0 + x_1 i + x_2 j + x_3 ij = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}.$$

Neste caso, temos as seguintes regras:

$$i^2 = j^2 = k^2 = -1,\ \ ij = k,\ \ ji = -k,\ \ jk = i,\ \ kj = -i,\ \ ki = j \text{ e } ik = -j.$$

Portanto,

$$N(\alpha) = \alpha\overline{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Registramos isto no seguinte Lema que também é conhecido como a Identidade de Lagrange.

Lema 2.1 (Identidade de Lagrange) *Se $x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3 \in \mathbb{R}$, então*

$$\begin{aligned}\left(\sum_{i=0}^{3} x_i^2\right)\left(\sum_{j=0}^{3} y_j^2\right) &= \left(\sum_{i=0}^{3} x_i y_i\right)^2 \\ &+ (x_0 y_1 - x_1 y_0 + x_2 y_3 - x_3 y_2)^2 \\ &+ (x_0 y_2 - x_2 y_0 + x_3 y_1 - x_1 y_3)^2 \\ &+ (x_0 y_3 - x_3 y_0 + x_1 y_2 - x_2 y_1)^2\end{aligned}$$

■

2.2 Inteiros de Hurwitz

O anel dos quatérnios de Hurwitz $\mathbb{Z}_H$ é o $\mathbb{Z}$-módulo

$$\mathbb{Z}_H = \left\{x_0 + x_1 i + x_2 j + x_3 k : \text{ ou } x_i \in \mathbb{Z}, \forall i \text{ ou } x_i \in \mathbb{Z} + \frac{1}{2}, \forall i\right\}.$$

Lema 2.2 *Seja $\alpha \in \mathbb{Z}_H$ com $\alpha \neq 0$. Então $\overline{\alpha} \in \mathbb{Z}_H$ e $N(\alpha) \in \mathbb{N}$.*

Prova. Seja $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{Z}_H$ com $\alpha \neq 0$. Então há dois casos a ser considerado:

1.^{o} **Caso**. Se $x_0, x_1, x_2, x_3 \in \mathbb{Z}$, então

$$N(\alpha) = x_0^2 + x_1^2 + x_2^2 + x_3^2 \in \mathbb{N}.$$

2.^{o} **Caso**. Se $x_0, x_1, x_2, x_3 \in \mathbb{Z} + \frac{1}{2}$, então

$$\begin{aligned} N(\alpha) &= x_0^2 + x_1^2 + x_2^2 + x_3^2 \\ &= \left(y_0 + \frac{1}{2}\right)^2 + \left(y_1 + \frac{1}{2}\right)^2 + \left(y_2 + \frac{1}{2}\right)^2 + \left(y_3 + \frac{1}{2}\right)^2 \\ &= \left(y_0^2 + y_1^2 + y_2^2 + y_3^2\right) + (y_0 + y_1 + y_2 + y_3) + 1 \in \mathbb{N}. \end{aligned}$$

Portanto, em qualquer caso, $N(\alpha) \in \mathbb{N}$. ■

Seja $\alpha \in \mathbb{Z}_H$. Dizemos que α é *ímpar* se $N(\alpha)$ é inteiro ímpar, caso contrário, dizemos que α é *par*.

Teorema 2.3 *Seja $\mathbb{Z}_H$ o anel dos inteiros de $\mathbb{H}$.*

1. *$\alpha \in U(\mathbb{Z}_H)$ se, e somente se, $N(\alpha) = 1$.*

2. $$U(\mathbb{Z}_H) = \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}.$$

   Assim, $|U(\mathbb{Z}_H)| = 24$.

3. *$\mathbb{Z}_H = \mathbb{Z}[\rho, i, j, k]$, onde $\rho = \frac{1}{2}(1 + i + j + k)$.*

Prova. 1. Seja $\alpha \in U(\mathbb{Z}_H)$. Então existe $\beta = \alpha^{-1} \in U(\mathbb{Z}_H)$ tal que $\alpha\beta = \beta\alpha = 1$. Logo, pelo Lema 2.2,

$$N(\alpha)N(\beta) = N(\alpha\beta) = 1$$

implica que $N(\alpha) = 1$. Reciprocamente, se $\alpha \in \mathbb{Z}_H$ e $N(\alpha) = 1$, então

$$1 = N(\alpha) = \alpha\overline{\alpha}.$$

Portanto, $\alpha^{-1} = \overline{\alpha} \in \mathbb{Z}_H$ e $\alpha \in U(\mathbb{Z}_H)$.

2. Seja $\alpha = x_0 + x_1 i + x_2 j + x_3 k \in U(\mathbb{Z}_H)$. Então

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 1.$$

Logo, se $x_0, x_1, x_2, x_3 \in \mathbb{Z}$, então

$$x_l = \pm 1 \text{ e } x_m = 0 \text{ se } l \neq m.$$

Por exemplo, se $x_0 = \pm 1$, então $x_1 = x_2 = x_3 = 0$. Logo,

$$(\pm 1)^2 + 0^2 + 0^2 + 0^2 = 1.$$

Agora, se $x_0, x_1, x_2, x_3 \in \mathbb{Z} + \frac{1}{2}$, então

$$x_0 = \pm\frac{1}{2},\ \ x_1 = \pm\frac{1}{2},\ \ x_2 = \pm\frac{1}{2} \text{ e } x_3 = \pm\frac{1}{2},$$

ou seja,

$$\left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 = 1.$$

Portanto,

$$U(\mathbb{Z}_H) = \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}.$$

3. Para cada $\alpha \in \mathbb{Z}_H$, podemos escrevê-lo do seguinte modo

$$\begin{aligned}
\alpha &= (a_0 + \frac{1}{2}) + (a_1 + \frac{1}{2})i + (a_2 + \frac{1}{2})j + (a_3 + \frac{1}{2})k \\
&= a_0 + \frac{1}{2} + a_1 i + \frac{1}{2}i + a_2 j + \frac{1}{2}j + a_3 k + \frac{1}{2}k \\
&= a_0 + \frac{1}{2}(1 + i + j + k) + a_1 i + a_2 j + a_3 k \\
&= a_0 + \rho + a_1 i + a_2 j + a_3 k \\
&= x_0\rho + x_1 i + x_2 j + x_3 k,
\end{aligned}$$

onde $x_0 = (a_0\rho^{-1} + 1), x_1 = a_1, x_2 = a_2, x_3 = a_3 \in \mathbb{Z}$ pois a_0 é par. Assim, qualquer elemento desta forma pertence a $\mathbb{Z}_H$. Consideremos, agora um elemento $\beta \in \mathbb{Z}[\rho, i, j, k]$, onde

$$\begin{aligned}
\beta &= b_0\rho + b_1 i + b_2 j + b_3 k, \text{ onde } b_0, b_1, b_2, b_3 \in \mathbb{Z} \\
&= b_0\frac{1}{2}(1 + i + j + k) + b_1 i + b_2 j + b_3 k \\
&= \frac{1}{2}b_0 + (b_1 + \frac{1}{2})i + (b_2 + \frac{1}{2})j + (b_3 + \frac{1}{2})k.
\end{aligned}$$

Logo, $\beta \in \mathbb{Z}_H$. Portanto, $\mathbb{Z}_H = \mathbb{Z}[\rho, i, j, k]$. ■

Sejam $\alpha \in \mathbb{Z}_H$ e $\omega \in U(\mathbb{Z}_H)$. Os elementos $\alpha\omega$ e $\omega\alpha$ são chamados *associados* de α. Note que elementos associados tem normas iguais, pois

$$N(\alpha\omega) = N(\alpha)N(\omega) = N(\alpha).$$

Sejam $\alpha, \beta, \gamma \in \mathbb{Z}_H$ tais que $\gamma = \alpha\beta$. Dizemos que γ tem α como um *divisor à esquerda* e β como um *divisor à direita.*

Lema 2.4 *Seja $\alpha \in \mathbb{Z}_H$. Então pelo menos um de seus associados tem coordenadas inteiras. Se α é ímpar, então pelo menos um de seus associados tem coordenadas não inteiras.*

Prova. Se α tem coordenadas não inteiras, digamos

$$\begin{aligned}\alpha &= \left(x_0 \pm \frac{1}{2}\right) + \left(x_1 \pm \frac{1}{2}\right) i + \left(x_2 \pm \frac{1}{2}\right) j + \left(x_3 \pm \frac{1}{2}\right) k \\ &= x_0 \pm \frac{1}{2} + x_1 i \pm \frac{1}{2} i + x_2 j \pm \frac{1}{2} j + x_3 k \pm \frac{1}{2} k \\ &= (x_0 + x_1 i + x_2 j + x_3 k) + \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \\ &= \beta + \gamma\end{aligned}$$

onde x_0, x_1, x_2, x_3 são números pares, então

$$\beta = (x_0 + x_1 i + x_2 j + x_3 k),$$

tem coordenadas inteiras. Assim, qualquer associado de β tem coordenadas inteiras. Como

$$\gamma = \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \in U(\mathbb{Z}_H)$$

temos que 1 é um associado de γ. Logo,

$$\alpha\overline{\gamma} = [\beta + \gamma]\overline{\gamma}$$

é um associado de α com coordenadas inteiras. Agora, se α é ímpar e tem coordenadas inteiras, digamos

$$\alpha = (x_0 + x_1 i + x_2 j + x_3 k) + (y_0 + y_1 i + y_2 j + y_3 k) = \beta + \gamma,$$

onde x_0, x_1, x_2, x_3 são números pares e

$$y_0, y_1, y_2, y_3 \in \{0, 1\},$$

com um deles é igual 1 ou três deles iguais a 1, pois $N(\alpha)$ é ímpar. Como as coordenadas de

$$\beta = x_0 + x_1 i + x_2 j + x_3 k$$

são inteiras temos que os associados de β tem coordenadas inteiras. Assim, basta mostrar que cada um dos elementos

$$1,\ \ i,\ \ j,\ \ k,\ \ 1 + i + j,\ \ 1 + i + k,\ \ 1 + j + k,\ \ i + j + k$$

tem um dos associados com coordenadas não inteiras. Por exemplo, se $\gamma = i$, então

$$\gamma\rho = i\frac{1}{2}(1 + i + j + k)$$

tem coordenadas não inteiras. Se

$$\gamma = 1+j+k = (1+i+j+k)-i = \lambda+\mu \text{ ou } \gamma = i+j+k = (1+i+j+k)-1 = \lambda+\mu,$$

então

$$\begin{aligned}\lambda\omega &= \lambda\frac{1}{2}(1-i-j-k)\\ &= (1+i+j+k)\frac{1}{2}(1-i-j-k)\\ &= 2\end{aligned}$$

e as coordenadas de $\mu\omega$ não são inteiras. ■

Lema 2.5 *Sejam $\kappa \in \mathbb{Z}_H$ e $m \in \mathbb{Z}$. Então existe $\lambda \in \mathbb{Z}_H$ tal que*

$$N(\kappa - m\lambda) < m^2 = N(m).$$

Prova. Para $m = 1$ nada há para ser provado. Suponhamos que $m > 1$.Consideremos

$$\kappa = x_0\rho + x_1 i + x_2 j + x_3 k \text{ e } \lambda = y_0\rho + y_1 i + y_2 j + y_3 k,$$

onde $x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3 \in \mathbb{Z}$. Assim,

$$\begin{aligned}\kappa - m\lambda &= x_0\rho + x_1 i + x_2 j + x_3 k - m(y_0\rho + y_1 i + y_2 j + y_3 k)\\ &= x_0\frac{1}{2}(1+i+j+k) + x_1 i + x_2 j + x_3 k - m(\frac{1}{2}(1+i+j+k) + y_1 i + y_2 j + y_3 k)\\ &= \frac{1}{2}(x_0 - my_0) + \frac{1}{2}(x_0 + 2x_1 - m(y_0 + 2y_1))\, i\\ &\quad + \frac{1}{2}(x_0 + 2x_2 - m(y_0 + 2y_2))\, j\\ &\quad + \frac{1}{2}(x_0 + 2x_3 - m(y_0 + 2y_3))\, k\end{aligned}$$

Provaremos abaixo que podemos escolher $y_0, y_1, y_2, y_3 \in \mathbb{Z}$ tal que

$$\begin{aligned} |x_0 - my_0| < \tfrac{m}{2}, &\qquad |x_0 + 2x_1 - m(y_0 + 2y_1)| < m,\\ |x_0 + 2x_2 - m(y_0 + 2y_2)| < m, &\quad |x_0 + 2x_3 - m(y_0 + 2y_3)| < m.\end{aligned}$$

1. Existe um inteiro y_0 tal que $x_0 = my_0 + r$, onde $-\frac{m}{2} \leq r \leq \frac{m}{2}$; assim, para este y_0, $|x_0 - my_0| = |r| \leq \frac{m}{2}$.

2. Existe um inteiro k tal que

$$x_0 + 2y_1 = km + r \text{ e } 0 \leq r < m.$$

Se $k - x_0$ é par, então $2y_1 = k - x_0$; assim, $x_0 + 2y_1 = (2y_1 + x_0)m + r$ e

$$|x_0 + 2x_1 - m\,(y_0 + 2y_1)| = r < m.$$

Por outro lado, se $k - y_0$ é ímpar, então $2y_1 = k - x_0 + 1$; assim, $x_0 + 2y_1 = (2y_1 + x_0 - 1)m + r = (2y_1 + x_0)m + r - m$ e

$$|x_0 + 2x_1 - m\,(y_0 + 2y_1)| = |r - m| \leq m,$$

pois $0 \leq r < m$. Logo, podemos determinar um inteiro y_1 satisfazendo

$$|x_0 + 2x_1 - m\,(y_0 + 2y_1)| \leq m.$$

3. Como em 2. podemos determinar um inteiro y_2 e y_3 satisfazendo

$$|x_0 + 2x_2 - m\,(y_0 + 2y_2)| \leq m \text{ e } |x_0 + 2x_3 - m\,(y_0 + 2y_3)| \leq m.$$

Portanto, obtemos

$$N\,(\kappa - m\lambda) \leq \frac{1}{16}m^2 + 3 \cdot \frac{1}{4}m^2 = \frac{13}{16}m^2 < m^2 = N(m).$$

■

Teorema 2.6 (Algoritmo da Divisão à direita) *Sejam $\alpha, \beta \in \mathbb{Z}_H$ com $\beta \neq 0$. Então existem $q, r \in \mathbb{Z}_H$ tais que*

$$\alpha = q\beta + r, \text{ onde } r = 0 \text{ ou } N(r) < N(\beta).$$

Prova. Pelo Lema 2.2, $N(\beta) \in \mathbb{N}$, digamos $m = N(\beta)$, então pelo Lema 2.5, existe $q \in \mathbb{Z}_H$ tal que

$$\alpha\overline{\beta} = mq + r_1 \text{ onde } N(r_1) < N(m).$$

Assim,

$$N(\alpha\overline{\beta} - mq) < N(m),$$

mas como $m = \beta\overline{\beta}$, obtemos

$$N\left(\alpha\overline{\beta} - \beta\overline{\beta}q\right) < N\,(m) \Rightarrow N((\alpha - q\beta)\,\overline{\beta}) < N(\beta)N(\overline{\beta}).$$

Como $N(\overline{\beta}) > 0$ temos que

$$N\,(\alpha - q\beta) < N(\beta).$$

Portanto, escolhendo $r = \alpha - q\beta \in \mathbb{Z}_H$ temos que

$$\alpha = q\beta + r, \text{ onde } r = 0 \text{ ou } 0 < N(r) < N(\beta).$$

■

Sejam $\alpha, \beta \in \mathbb{Z}_H$ com $\alpha \neq 0$ ou $\beta \neq 0$. O *máximo divisor comum à direita* de α e β, em símbolos $\text{mdc}_d(\alpha, \beta)$, é um elemento $\delta \in \mathbb{Z}_H$ tal que

1. δ é um divisor comum à direita de α e β;

2. Se γ é um divisor comum à direita de α e β, então γ é um divisor à direita de δ.

Teorema 2.7 *$\mathbb{Z}_H$ é um domínio principal à direita.*

Prova. Seja I um ideal à direita de $\mathbb{Z}_H$. Se $I = \{0\}$, nada há para ser provado. Suponhamos que $I \neq \{0\}$. Então o conjunto

$$X = \{N(\beta) \in \mathbb{N} : \beta \in I - \{0\}\}$$

é não-vazio. Assim, X possui um menor elemento, digamos $m \in X$. Seja $\alpha \in I - \{0\}$ tal que $N(\alpha) = m$.

Afirmação. $I = \langle\alpha\rangle = \{\lambda\alpha : \lambda \in \mathbb{Z}_H\}$.
De fato, é claro que $\langle\alpha\rangle \subseteq I$. Por outro lado, se $\gamma \in I$, então existem $q, r \in \mathbb{Z}_H$ tais que

$$\gamma = q\alpha + r, \text{ onde } r = 0 \text{ ou } N(r) < N(\alpha).$$

Suponhamos, por absurdo, que $r \neq 0$. Então

$$r = \gamma - q\alpha \in I \text{ com } 0 < N(r) < N(\alpha) = m,$$

o que é uma contradição. Logo, $\gamma = q\alpha \in \langle\alpha\rangle$, conseqüentemente $I \subseteq \langle\alpha\rangle$. Portanto, $I = \langle\alpha\rangle$. ■

Teorema 2.8 *Sejam $\alpha, \beta \in \mathbb{Z}_H$ com $\alpha \neq 0$ ou $\beta \neq 0$. Então $\delta = \text{mdc}_d(\alpha, \beta)$ existe e é, a menos de associados, único. Além disso, existem $\lambda, \mu \in \mathbb{Z}_H$ tais que*

$$\delta = \lambda\alpha + \mu\beta.$$

Prova. É fácil verificar que o conjunto

$$I = \langle \alpha, \beta \rangle = \{\lambda\alpha + \mu\beta : \lambda, \mu \in \mathbb{Z}_H\}$$

é um ideal à direita de $\mathbb{Z}_H$ com $I \neq \{0\}$. Assim, pelo Teorema 2.7, existe $\delta \in \mathbb{Z}_H$ tal que $I = \langle \delta \rangle$. Como $\delta \in I$ temos que existem $\lambda, \mu \in \mathbb{Z}_H$ tais que

$$\delta = \lambda\alpha + \mu\beta.$$

Afirmação. $\delta = \text{mdc}_d(\alpha, \beta)$.
De fato, como $\alpha, \beta \in I = \langle \delta \rangle$ temos que δ é um divisor comum à direita de α e β. Por outro lado, se δ' é um divisor comum à direita de α e β, então existem $\lambda', \mu' \in \mathbb{Z}_H$ tais que $\alpha = \lambda'\delta'$ e $\beta = \mu'\delta'$. Assim,

$$\delta = \lambda\alpha + \mu\beta = (\lambda\lambda' + \mu\mu')\delta'.$$

Portanto, δ' é um divisor à direita de δ. ■

Note que se δ é uma unidade ω, então todos os divisores comum à direita de α e β são unidades. Neste caso

$$\lambda\alpha + \mu\beta = \omega \Rightarrow (\omega^{-1}\lambda)\alpha + (\omega^{-1}\mu)\beta = 1.$$

Portanto, $\text{mdc}_d(\alpha, \beta) = 1$.

Sejam $\alpha, \beta \in \mathbb{Z}_H$ com $\alpha \neq 0$ e $\beta \neq 0$. Dizemos que α e β são *relativamente primos à direita* ou *primos entre si à direita* se $\text{mdc}_d(\alpha, \beta) = 1$.

Teorema 2.9 *Sejam $\alpha \in \mathbb{Z}_H$ e $\beta = m \in \mathbb{N}$. Então $\text{mdc}_d(\alpha, m) = 1$ se, e somente se, $\text{mdc}(N(\alpha), m) = 1$.*

Prova. Suponhamos que $\text{mdc}_d(\alpha, m) = 1$. Então existem $\lambda, \mu \in \mathbb{Z}_H$ tais que

$$1 = \lambda\alpha + \mu m.$$

Logo,

$$N(\lambda\alpha) = N(1 - \mu m) = (1 - m\mu)(1 - m\overline{\mu}).$$

Como $N(\lambda\alpha) = N(\lambda)N(\alpha)$ temos que

$$N(\lambda)N(\alpha) + (\mu + \overline{\mu} - N(\mu)m)m = 1.$$

Assim, $\mathrm{mdc}_d(N(\alpha), m) = 1$. Reciprocamente, se $\delta = \mathrm{mdc}_d(\alpha, m) \in \mathbb{Z}_H$, então existem $\lambda, \mu \in \mathbb{Z}_H$ tais que $\alpha = \lambda\delta$ e $m = \mu\delta$. Assim, $N(\delta)$ é um divisor comum de $N(\alpha)$ e $N(m)$, respectivamente. Portanto, $N(\delta)$ é um divisor de 1, isto é, $\delta \in U(\mathbb{Z}_H)$. Logo,

$$\lambda\alpha + \mu m = \delta \Rightarrow (\delta^{-1}\lambda)\alpha + (\delta^{-1}\mu)m = 1.$$

Portanto, $\mathrm{mdc}_d(\alpha, m) = 1$. ■

1. Um elemento $\pi \in \mathbb{Z}_H$ é *elemento primo* sobre $\mathbb{Z}_H$ se as seguintes condições são satisfeitas:

2. $\pi \notin U(\mathbb{Z}_H)$;

3. Se $\pi = \alpha\beta$, então $\alpha \in U(\mathbb{Z}_H)$ ou $\beta \in U(\mathbb{Z}_H)$.

Assim, os associados de um elemento primo são elementos primos. Além disso, se $\pi = \alpha\beta$, então

$$N(\pi) = N(\alpha\beta) = N(\alpha)\, N(\beta).$$

Logo se $N(\pi)$ for um número primo, emtão π é um elemento primo.

Corolário 2.10 *Seja p um número primo ímpar. Então existe um inteiro positivo k tal que $k < p$ e kp é soma de quatro quadrados.*

Prova. Pelo Lema 1.11 existem $x_0, y_0 \in \mathbb{Z}$ com

$$0 \leq x_0 \leq \frac{p-1}{2} \text{ e } 0 \leq y_0 \leq \frac{p-1}{2}$$

tais que

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp$$

para algum $k \in \mathbb{Z}$ e devemos ter $k > 0$. Logo,

$$kp = x_0^2 + y_0^2 + 1^2 < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2.$$

Portanto, $k < p$. ■

Lema 2.11 *Seja p um número primo em $\mathbb{N}$. Então p nunca é um elemento primo em $\mathbb{Z}_H$.*

Prova. Como

$$2 = (1+i)(1-i)$$

temos que 2 não é um elemento primo em $\mathbb{Z}_H$. Suponhamos que p é um número primo ímpar. Então, pelo Lema 1.11, existem inteiros $r, s \in \mathbb{Z}$ tais que

$$1 + r^2 + s^2 \equiv 0 \pmod{p} \text{ com } 0 < r, s < p.$$

Se

$$\alpha = 1 + si + rj \in \mathbb{Z}_H,$$

então

$$N(\alpha) = 1 + r^2 + s^2 \equiv 0 \pmod{p} \text{ e } \text{mdc}_d(N(\alpha), p) > 1,$$

pois $p \mid N(\alpha)$ e p é um número primo. Logo, pelo Teorema 2.9, existe $\delta \notin U(\mathbb{Z}_H)$ tal que $\delta = \text{mdc}_d(\alpha, p)$. Logo δ é um divisor comum à direita de α e de p, assim existem δ_1 e $\delta_2 \in \mathbb{Z}_H$ tais que

$$\alpha = \delta_1\delta \text{ e } p = \delta_2\delta,$$

mas δ_2 não pode ser uma unidade, caso contrário, δ seria um associado de p. Logo, p dividiria todas as coordenadas de

$$\alpha = \delta_1\delta = \delta_1\delta_2^{-1}p.$$

Em particular, p dividiria 1, pois se $p \mid 1$, p seria uma unidade. Portanto, $p = \delta_2\delta$, onde $\delta, \delta_2 \notin U(\mathbb{Z}_H)$, isto é, p não é um elemento primo em $\mathbb{Z}_H$. ■

Teorema 2.12 *Seja $\pi \in \mathbb{Z}_H$. Então π é um elemento primo se, e somente se, $N(\pi)$ é um número primo.*

Prova. Suponhamos que π seja um elemento primo e p um número primo que divide $N(\pi)$. Então, pelo Teorema 2.9, temos que existe $\pi' \notin U(\mathbb{Z}_H)$ tal que $\pi' = \text{mdc}_d(\pi, p)$. Por hipótese, então π' é um associado de π. Logo,

$$N(\pi) = N(\pi').$$

Além disso,

$$p = \lambda\pi' \text{ e } p^2 = N(\lambda)N(\pi') = N(\lambda)N(\pi).$$

Assim,

$$N(\lambda) = 1 \text{ ou } N(\lambda) = p.$$

Se $N(\lambda) = 1$, então p é um associado de π' e π, respectivamente. Logo, p é um elemento primo, o que é impossível, pelo Lema 2.5. Portanto, $N(\lambda) = p$ e assim

$$N(\pi) = p,$$

isto é, $N(\pi)$ é um número primo. Por outro lado, vimos que se $N(\pi)$ é um número primo, então π é um elemento primo. ■

2.3 Soma de Quatro Quadrados

Teorema 2.13 (Lagrange) *Todo inteiro positivo é soma de quatro quadrados.*

Prova. Pelo Lema 2.1 e o fato de que $1 = 1^2 + 0^2 + 0^2 + 0^2$, basta provar que todo número primo é soma de quatro quadrados, pois se n é qualquer inteiro, então basta fatorá-lo em fatores primos e usar a Identidade Lagrange. Assim, se $p = 2$, então

$$2 = 1^2 + 1^2 + 0^2 + 0^2.$$

Se p é um número primo ímpar, então pelo Corolário 2.10 existe um menor inteiro positivo $k \in \mathbb{Z}$ com $1 \leq k < p$ tal que

$$kp = x_0^2 + x_1^2 + x_2^2 + x_3^2, \text{ onde } x_0, x_1, x_2, x_3 \in \mathbb{Z}, \tag{2.1}$$

onde nem todos os x_i são divisíveis por p.

Afirmação. $k = 1$.

De fato, suponhamos, por absurdo, que $k > 1$. Se k é um número par, então

$$x_0^2 + x_1^2 + x_2^2 + x_3^2$$

também é um número par. Logo, temos as seguintes possibilidades:

1. x_0, x_1, x_2, x_3 são todos pares;
2. x_0, x_1, x_2, x_3 são todos ímpares;
3. x_0, x_1, x_2, x_3 dois são pares e dois são ímpares, digamos que x_0 e x_1 são pares e x_2 e x_3 são ímpares.

De qualquer forma, em todas as três possibilidades os números inteiros

$$x_0 + x_1, \;\; x_0 - x_1, \;\; x_2 + x_3, \;\; x_2 - x_3$$

são pares. Assim,

$$\frac{1}{2}kp = \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2,$$

é uma soma de quatro quadrados inteiros, o que é uma contradição, pois $\frac{1}{2}k < k$. Portanto, k é ímpar e $k \geq 3$. Como

$$\{0, 1, \ldots, k-1\} \text{ e } \{-\frac{k-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{k-1}{2}\}$$

são ambos sistemas de resíduos módulo k, podemos escolher $y_i \in \mathbb{Z}$, $i = 0, 1, 2, 3$, de modo que

$$y_i \equiv x_i \pmod{k} \text{ e } |y_i| < \frac{k}{2}, i = 0, 1, 2, 3.$$

Temos então

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 \equiv x_0^2 + x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod{k}$$

e, assim,

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 = k_1 k,$$

onde $k_1 > 0$, pois caso contrário

$$y_i = 0 \Rightarrow k \mid x_i \text{ para cada } i$$

e

$$k^2 \mid x_0^2 + x_1^2 + x_2^2 + x_3^2 \Rightarrow k^2 \mid kp \Rightarrow k \mid p$$

o que é uma contadição, pois $1 \leq k < p$. Além disso, devemos ter $k_1 < k$, pois

$$0 < k_1 k = y_0^2 + y_1^2 + y_2^2 + y_3^2 < 4\left(\frac{k}{2}\right)^2 = k^2. \tag{2.2}$$

Pela equações 2.1 e 2.2 segue, pela Identidade de Lagrange, que

$$k^2 k_1 p = (kp)(kk_1) = z_0^2 + z_1^2 + z_2^2 + z_3^2,$$

onde os z_i são as somas da direita. Logo,

$$z_0 = \sum_{i=0}^{3} x_i y_i = \sum_{i=0}^{3} x_i(x_i - a_i k) \equiv \sum_{i=0}^{3} x_i^2 \equiv 0 \pmod{k};$$

e para os outros três termos, observemos, duas vezes para cada termos, que

$$z_i = x_l x_m - x_m x_l \equiv x_l x_m - x_m x_l \equiv 0 \pmod{k}, i = 1, 2, 3.$$

E, existem $t_0, t_1, t_2, t_3 \in \mathbb{Z}$ tais que

$$z_0 = kt_0, \;\; z_1 = kt_1, \;\; z_2 = kt_2, \;\; z_3 = kt_3.$$

Então

$$k^2 k_1 p = z_0^2 + z_1^2 + z_2^2 + z_3^2 = k^2[t_0^2 + t_1^2 + t_2^2 + t_3^2].$$

Logo,

$$k_1 p = t_0^2 + t_1^2 + t_2^2 + t_3^2,$$

o que contradiz a minimalidade de k, pois $0 < k_1 < k$. ■

Teorema 2.14 (Hurwitz) *Todo inteiro positivo é soma de quatro quadrados.*

Prova. Pelo Lema 2.1 e o fato de que $1 = 1^2 + 0^2 + 0^2 + 0^2$, basta provar que todo número primo é soma de quatro quadrados. Se $p = 2$, então

$$2 = 1^2 + 1^2 + 0^2 + 0^2.$$

Se p um número primo ímpar, então pelo Lema 2.11, existem $\lambda, \pi \in \mathbb{Z}_H$ tais que

$$p = \lambda\pi, \;\; \text{onde} \;\; N(\lambda) = N(\pi) = p.$$

Se π tem coordenadas $x_0, x_1, x_2, x_3 \in \mathbb{Z}$, então

$$p = N(\pi) = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Se as coordenadas de π não são inteiras, então pelo Lema 2.4, existe um associado π' de π com coordenadas inteiras e, assim,

$$p = N(\pi) = N(\pi') = y_0^2 + y_1^2 + y_2^2 + y_3^2.$$

Portanto, em qualquer caso p é soma de quatro quadrados. ■

Proposição 2.15 *Se p é um número primo ímpar, então $4p$ é a soma de quatro quadrados ímpares.*

Prova. Pelo Lema 2.11 existem $\lambda, \pi \in \mathbb{Z}_H$ tais que

$$p = \lambda\pi, \text{ onde } N(\lambda) = N(\pi) = p.$$

Assim, pelo Lema 2.4, podemos escolher um associado π' de π cujas coordenadas são metade de inteiros ímpares, isto é,

$$p = N(\pi) = N(\pi') = \left(y_0 + \frac{1}{2}\right)^2 + \left(y_1 + \frac{1}{2}\right)^2 + \left(y_2 + \frac{1}{2}\right)^2 + \left(y_3 + \frac{1}{2}\right)^2,$$

onde $y_0, y_1, y_2, y_3 \in \mathbb{Z}$ e

$$4p = (2y_0 + 1)^2 + (2y_1 + 1)^2 + (2y_2 + 1)^2 + (2y_3 + 1)^2.$$

Por exemplo,

$$4 \cdot 3 = 12 = 1^2 + 1^2 + 1^2 + 3^2,$$

mas, $4 \cdot 2 = 8$ não é soma de quatro quadrados ímpares. ■

Capítulo 3

Teorema de Cohn em Soma de Quatro Quadrados

Neste capítulo definiremos o anel de quatérnios Cubianos e exibiremos algumas de suas propriedades. E mostraremos, através da combinação de resultados da geometria de números e do anel de quatérnios Cubianos, que todo inteiro algébrico totalmente positivo com coeficiente par no termo radical é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$.

3.1 Inteiros Cubianos

O anel dos quatérnios cubianos $\mathbb{Z}_C$ é o $\mathbb{Z}[\sqrt{2}]$-módulo

$$\mathbb{Z}_C = \mathbb{Z}[\sqrt{2}][1, \rho_1, \rho_2, \rho_3],$$

onde

$$\rho_1 = \frac{\sqrt{2}}{2}(1+i), \;\; \rho_2 = \frac{\sqrt{2}}{2}(1+j) \;\text{ e }\; \rho_3 = \rho = \frac{1}{2}(1+i+j+k).$$

Lema 3.1 *Seja $\mathbb{Z}_C$ o anel cubiano de $\mathbb{H}$. Então*

$$U(\mathbb{Z}_C) = U(\mathbb{Z}_H) \cup \left\{ \frac{\sqrt{2}}{2}(\pm x \pm y) : x, y \in \{1, i, j, k\} \;\; com \;\; x \neq y \right\}.$$

Assim, $|U(\mathbb{Z}_C)| = 48$.

Prova. Seja

$$\lambda = \frac{\sqrt{2}}{2}(\pm x \pm y) \in \mathbb{Z}_C.$$

Então

$$N(\lambda) = \left(\frac{\sqrt{2}}{2}x\right)^2 + \left(\frac{\sqrt{2}}{2}y\right)^2 = \frac{1}{2}(|x|^2 + |y|^2) = 1,$$

pois $x, y \in \{1, i, j, k\}$ com $x \neq y$. ■

Observação 3.2 *Enquanto os inteiros de Hurwitz tem associados com coeficientes inteiros na base* $\{1, i, j, k\}$*, os inteiros cubianos tem associados com coeficientes em* $\mathbb{Z}[\sqrt{2}]$ *nesta base.*

Lema 3.3 *Seja* $\mathbb{Z}_C$ *o anel cubiano de* $\mathbb{H}$*. Então* $\mathbb{Z}_C \cap \mathbb{R} = \mathbb{Z}[\sqrt{2}]$.

Prova. Como $1 \in \mathbb{Z}_C$ temos que

$$\sqrt{2} = 1\sqrt{2} \in \mathbb{Z}_C.$$

Logo, $\mathbb{Z}[\sqrt{2}] \subseteq \mathbb{Z}_C \cap \mathbb{R}$. Por outro lado, seja

$$\lambda = x_0 + x_1\rho_1 + x_2\rho_2 + x_3\rho_3 \in \mathbb{Z}_C \cap \mathbb{R}.$$

Então

$$\begin{aligned}
\lambda &= x_0 + x_1\left(\frac{\sqrt{2}}{2}(1+i)\right) + x_2\left(\frac{\sqrt{2}}{2}(1+j)\right) + x_3\left(\frac{1}{2}(1+i+j+k)\right) \\
&= x_0 + \frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}}{2}x_1 i + \frac{\sqrt{2}}{2}x_2 + \frac{\sqrt{2}}{2}x_2 j + \frac{1}{2}x_3 + \frac{1}{2}x_3 i + \frac{1}{2}x_3 j + \frac{1}{2}x_3 k \\
&= \left(x_0 + \frac{1}{2}x_3\right) + \left(\frac{x_1 + x_2}{2}\right)\sqrt{2} + \left(\frac{\sqrt{2}}{2}x_1 + \frac{1}{2}x_3\right)i + \left(\frac{\sqrt{2}}{2}x_2 + \frac{1}{2}x_3\right)j + \frac{1}{2}x_3 k.
\end{aligned}$$

Como $\lambda \in \mathbb{R}$ temos que $x_1 = x_2 = x_3 = 0$. Logo,

$$\lambda = x_0 \in \mathbb{Z}[\sqrt{2}].$$

Portanto, $\mathbb{Z}_C \cap \mathbb{R} \subseteq \mathbb{Z}[\sqrt{2}]$. ■

Corolário 3.4 *Se* $\alpha \in \mathbb{Z}_C$*, então* $N(\alpha), \mathrm{tr}(\alpha) \in \mathbb{Z}[\sqrt{2}]$.

Prova. Se $\alpha \in \mathbb{Z}_C$, então $N(\alpha) \in \mathbb{Z}_C \cap \mathbb{R} = \mathbb{Z}[\sqrt{2}]$ e $\mathrm{tr}(\alpha) \in \mathbb{Z}_C \cap \mathbb{R} = \mathbb{Z}[\sqrt{2}]$. ■

Lema 3.5 *Para cada elemento* $\lambda \in \mathbb{Z}_C$ *existe um elemento* $\omega \in U(\mathbb{Z}_C)$ *tal que*

$$\sqrt{2}\lambda\omega \in \mathbb{Z}[\sqrt{2}]\,[1, i, j, k]\,.$$

Prova. Vamos mostrar o Lema apenas para os elementos da Tabela abaixo. O caso geral pode ser encontrado em [1, Lemma 6, p 268].

$$\begin{array}{ccc} \lambda \in \mathbb{Z}_C & \omega \in U(\mathbb{Z}_C) & \sqrt{2}\lambda\omega \in \mathbb{Z}[\sqrt{2}]\,[1,i,j,k] \\ \sqrt{2}\cdot 1 & 1 & 2 \\ \sqrt{2}\cdot 1 + (\sqrt{2}+1)\rho_2 & \rho_1 & \sqrt{2} + (1+2\sqrt{2})i + (1+\sqrt{2})j \\ \sqrt{2}\cdot 1 + \rho_2 & 1 & 3 + j. \end{array}$$

■

Lema 3.6 *Seja $\lambda \in \mathbb{Z}_C$ com $N(\lambda) = a + b\sqrt{2}$, onde a é um número ímpar e b um número par. Então existe um elemento $\omega \in U(\mathbb{Z}_C)$ tal que*

$$\lambda\omega \in \mathbb{Z}[\sqrt{2}]\,[1,i,j,k]\,.$$

Prova. Pode-se verificar que os elementos da Tabela abaixo podem ser usados para provar o Lema. Para uma prova detalhada pode consultar [1, Lemma 7, p 269].

$$\begin{array}{ccc} \lambda \in \mathbb{Z}_C & \omega \in U(\mathbb{Z}_C) & \lambda\omega \in \mathbb{Z}[\sqrt{2}]\,[1,i,j,k] \\ 1+\rho_3 & \rho_3 & i+j+k \\ 1+\sqrt{2}\rho_2 & 1 & 2+j \\ 1+\sqrt{2}\rho_1 & 1 & 2+i. \end{array}$$

■

Observação 3.7 *Note que $\mathbb{Z}[\sqrt{2}]\,[1,i,j,k]$ está contido propriamente em $\mathbb{Z}_C$, pois*

$$\begin{aligned} 1 &\in \mathbb{Z}_C,\ i = \sqrt{2}\rho_1 - 1 \in \mathbb{Z}_C,\ j = \sqrt{2}\rho_2 - 1 \in \mathbb{Z}_C \ \ e \\ k &= 2\rho_3 - 1 - i - j \in \mathbb{Z}_C. \end{aligned}$$

Mas

$$\rho_1 = \frac{\sqrt{2}}{2}(1+i) \in \mathbb{Z}_C \ \ e \ \ \rho_1 \notin \mathbb{Z}[\sqrt{2}]\,[1,i,j,k]\,.$$

Lema 3.8 *Seja $\pi \in \mathbb{Z}[\sqrt{2}]$ um elemento primo. Então existem $\omega \in U(\mathbb{Z}[\sqrt{2}])$ e $\lambda \in \mathbb{Z}_C$ tais que*

$$N(\lambda) = \omega\pi$$

Prova. Se $\pi \in \mathbb{Z}[\sqrt{2}]$ é um elemento primo, então existe um único primo $p \in \mathbb{Z}$ tal que π está acima de p. Temos três casos a serem considerados:

1.^{o} **Caso**. Se p é inerte, então

$$\pi = \tau p, \text{ onde } \tau \in U(\mathbb{Z}[\sqrt{2}]).$$

Consideremos $\omega = \tau^{-1}$. Temos, assim, o caso clássico, onde $p = a^2 + b^2 + c^2 + d^2$, com $a, b, c, d \in \mathbb{Z}$. Fazendo $\lambda = a + bi + cj + dk \in \mathbb{Z}_C$, obtemos

$$N(\lambda) = a^2 + b^2 + c^2 + d^2 = p = \omega\pi.$$

2.^{o} **Caso**. Se p ramifica, então

$$\pi = \tau\sqrt{2}.$$

Seja $\beta = 1 + \rho_1$. Assim

$$N(\beta) = 2 + \sqrt{2} = \sqrt{2}(1 + \sqrt{2}).$$

Consideremos $\tau = 1+\sqrt{2}$, obtemos $N(\tau) = -1$. Logo, $\tau \in U(\mathbb{Z}[\sqrt{2}])$ e $\tau^{-1} = -1+\sqrt{2} > 0$. Agora, se $\lambda = \tau^{-1}\beta$, então

$$N(\lambda) = N(\tau^{-1}\beta) = N(\tau^{-1})N(\beta) = \tau^{-1}N(\beta) = \tau^{-1}\tau\sqrt{2} = \sqrt{2}.$$

Portanto,

$$N(\lambda) = \sqrt{2} = \tau^{-1}\pi, \text{ para } \omega = \tau^{-1}.$$

3.^{o} **Caso**. Se p decompõe-se, então pelo Lema (1.13), existe $\kappa, \alpha, \beta, \gamma, \delta \in \mathbb{Z}[\sqrt{2}]$ tais que $\kappa\pi = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$ com $|\kappa\overline{\kappa}| \leq 9$. Suponhamos que $|\pi\overline{\pi}| > 9$. Consideremos

$$\widehat{\lambda} = \alpha + \beta i + \gamma j + \delta k \in \mathbb{Z}_C, \text{ onde } N(\widehat{\lambda}) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = \kappa\pi$$

e

$$\pi i \in \mathbb{Z}_C, \text{ onde } N(\pi i) = \pi^2.$$

Como $\mathbb{Z}_C$ é um domínio principal à direita temos que existe um elemento $r \in \mathbb{Z}_C$ tal que

$$r\mathbb{Z}_C = \langle r \rangle = \langle \pi i, \widehat{\lambda} \rangle.$$

Assim, existem $s, t \in \mathbb{Z}_C$ tais que $r = s\pi i + t\widehat{\lambda}$. Por outro lado, existem $v_1, v_2 \in \mathbb{Z}_C$ tais que $\pi i = v_1$ e $r\widehat{\lambda} = v_2 r$. Assim,

$$N(v_1 r) = \pi^2 \text{ e } N(v_2 r) = \kappa\pi \Rightarrow N(r) \mid \pi^2 \text{ e } N(r) \mid \kappa\pi.$$

Como $|\kappa\overline{\kappa}| \leq 9 < |\pi\overline{\pi}|$ temos que $\mathrm{mdc}_d(\kappa, \pi) = 1$. Logo, $N(r) = \pm 1$ ou $N(r) = \tau\pi$, onde $\tau \in U(\mathbb{Z}[\sqrt{2}])$. Sendo

$$N(r) = r\overline{r} = \pi\widehat{s} + N(\widehat{\lambda})N(t)$$

e $N(r), N(t), N(\widehat{\lambda}) \in \mathbb{R}$ temos que $\widehat{s} \in \mathbb{R}$ e pelo Lema 3.4 $\widehat{s} \in \mathbb{Z}[\sqrt{2}]$.

$$\begin{aligned} N(r) &= r\overline{r} = \pi\widehat{s} + N(\widehat{\lambda})N(t). \\ &= \pi[\widehat{s} + \kappa N(t)], \end{aligned}$$

Então, $\pi \mid N(r)$. Logo, $N(r) \neq \pm 1$ e, assim, $N(r) = \tau\pi$. Neste caso, temos que r faz o papel de λ no enunciado do Lema.

Agora, vejamos o caso em que p se decompõe e $|\pi\overline{\pi}| \leq 9$. Notemos que se

$$\pi\overline{\pi} = 1, \text{ é uma unidade, não serve.}$$
$$\pi\overline{\pi} = 2, \text{ ramifica, já visto.}$$
$$\pi\overline{\pi} = 3, \text{ inerte, já visto.}$$
$$\pi\overline{\pi} = 4, \text{ ramifica, já visto.}$$
$$\pi\overline{\pi} = 5, \text{ inerte, já visto.}$$
$$\pi\overline{\pi} = 6, \text{ inerte e ramifica, não serve,}$$
$$\pi\overline{\pi} = 8, \text{ ramifica, já visto,}$$
$$\pi\overline{\pi} = 9, \text{ inerte, já visto}$$

então, a única possibilidade é $p = 7 = |\pi\overline{\pi}|$. Observemos que

$$N(\rho_1 + \sqrt{2}\rho_2) = 3 + \sqrt{2} \text{ e } (3 + \sqrt{2})(3 - \sqrt{2}) = 7.$$

Mas $7 \equiv -1 (\mathrm{mod}\, 8)$. Logo, pelo Lema (1.9),

$$3 + \sqrt{2} \text{ e } 3 - \sqrt{2}$$

são primos e são a menos de associados os únicos primos acima de 7. Como $|\pi\overline{\pi}| = 7$ temos que π é um associado de $3 + \sqrt{2}$ ou π é um associado de $3 - \sqrt{2}$. Ou seja,

$$\pi = \omega(3 + \sqrt{2}) \text{ ou } \pi = \omega(3 - \sqrt{2}) \text{ onde } \omega \in U(\mathbb{Z}[\sqrt{2}]).$$

Então,

$$\omega^{-1}\pi = N(\rho_1 + \sqrt{2}\rho_2) \text{ ou } \omega^{-1}\pi = N(\rho_1 - \sqrt{2}\rho_2).$$

Portanto, existem $\omega \in U(\mathbb{Z}[\sqrt{2}])$ e $\lambda \in \mathbb{Z}_C$ tais que

$$N(\lambda) = \omega\pi$$

■

Dizemos que um elemento $\pi \in \mathbb{Z}[\sqrt{d}]$ é *totalmente positivo* se π e $\overline{\pi}$ estiverem contidos em $\mathbb{R}_+$. Em nosso caso, temos que $\pi = a + b\sqrt{2}$, então

$$0 < a + b\sqrt{2} = \pi \text{ e } 0 < a - b\sqrt{2} = \overline{\pi}$$

são totalmente positivos.

Lema 3.9 *Para cada $q_i \in \mathbb{Z}[\sqrt{d}]$ que não é totalmente positivo, existe um $s_i \in \mathbb{N}$ tal que*

$$(1+\sqrt{2})^{s_i} q_i$$

é totalmente positivo.

Prova. Suponhamos que

$$q_i = a_i + b_i\sqrt{2}$$

não seja totalmente positivo e definimos

$$q_i' = \begin{cases} q_i(1+\sqrt{2}) & \text{se } q_i > 0 \\ q_i(1+\sqrt{2})^{-1} & \text{se } q_i < 0 \end{cases}$$

Afirmação. q_i' é totalmente positivo.

De fato, note que $q_i' > 0$

$$\overline{q_i'} = \begin{cases} \overline{q_i}(1+\sqrt{2}) & \text{se } q_i > 0 \Rightarrow \overline{q_i} < 0 \\ \overline{q_i}(1+\sqrt{2})^{-1} & \text{se } q_i < 0 \Rightarrow \overline{q_i} > 0 \end{cases}.$$

Logo, q_i' e $\overline{q_i'}$ são maiores que zero. Portanto, q_i' é totalmente positivo. ■

Lema 3.10 *Seja $\pi \in \mathbb{Z}[\sqrt{2}]$ elemento primo totalmente positivo que está acima de número primo p com $p \equiv 1 \pmod 8$. Então π pode ser escrito como a soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$.*

Prova. Seja $\pi = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Então

$$N(\pi) = a^2 - 2b^2 = p \equiv 1 \pmod 8,$$

isto implica que $a^2 - 2b^2$ é ímpar. Logo a^2 é ímpar pois $2b^2$ é par e, assim, b é par. Logo,

$$a \equiv 1 \pmod 2 \text{ e, portanto, } \pi = a + b\sqrt{2} \equiv 1 \pmod 2 \text{ em } \mathbb{Z}[\sqrt{2}].$$

Pelo Lema (3.8), temos que existe um elemento $\lambda \in \mathbb{Z}_C$ e um elemento $\omega \in U(\mathbb{Z}[\sqrt{2}])$ tal que $N(\lambda) = \omega\pi$. Consideremos

$$\lambda = \alpha + \beta i + \gamma j + \delta k \in \mathbb{Z}_C, \text{ com } \alpha, \beta, \gamma, \delta \in \frac{1}{2}\mathbb{Z}[\sqrt{2}].$$

Então

$$\omega\pi = N(\lambda) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 > 0$$

Obtemos, assim, que $\overline{\omega\pi}$ é soma de quatro quadrados e maior que zero. Logo, $\omega\pi$ é totalmente positivo. Mas como π é totalmente positivo mostraremos que ω também deve ser totalmente positivo. Se ω é totalmente positivo, então $\omega > 0$ e $\overline{\omega} > 0$. Temos que

$$\omega = \pm(1+\sqrt{2})^n, \ n \in \mathbb{Z}.$$

Se $2 \nmid n$, então

$$n = 2l + 1 \Rightarrow 0 < \omega = \pm[(1+\sqrt{2})^2]^l(1+\sqrt{2}) > 0.$$

Portanto, o sinal é positivo. Logo,

$$\overline{\omega} = [(1-\sqrt{2})^2]^l(1-\sqrt{2}) < 0,$$

o que é um absurdo. Logo,

$$0 < \omega = (1+\sqrt{2})^n, \ n \text{ par } \Rightarrow \text{ sinal é positivo } .$$

Portanto,

$$\omega = (1+\sqrt{2})^{2l}, \text{ onde } n = 2l.$$

E mais,

$$\begin{aligned} \omega &= (1+\sqrt{2})^{2l} = [(1+\sqrt{2})^2]^l \\ &= [1+2+2\sqrt{2}]^l \equiv 1 \pmod 2 \\ &\Rightarrow \omega \equiv 1 \pmod 2. \end{aligned}$$

Já que $\pi \equiv 1 \pmod 2$ e $\omega \equiv 1 \pmod 2$ em $\mathbb{Z}[\sqrt{2}]$ e $N(\lambda) = \omega\pi$. Portanto,

$$N(\lambda) \equiv 1 \pmod 2 \text{ em } \mathbb{Z}[\sqrt{2}].$$

Pelo Lema 3.6, existe $\omega \in U(\mathbb{Z}_C)$ tal que $\lambda\omega \in \mathbb{Z}[\sqrt{2}]\,[1,i,j,k]$. Seja $\lambda\omega = \widehat{\alpha} + \widehat{\beta}i + \widehat{\gamma}j + \widehat{\delta}k$ e como $n = 2l$ e

$$(1+\sqrt{2})^n\pi = N(\lambda) = N(\lambda\omega) = (\widehat{\alpha})^2 + (\widehat{\beta})^2 + (\widehat{\gamma})^2 + (\widehat{\delta})^2.$$

Dividindo os dois lados desta igualdade por $(1+\sqrt{2})^n$, obtemos

$$\begin{aligned}\pi &= \left[\frac{(\widehat{\alpha})^2}{(1+\sqrt{2})^n}+\frac{(\widehat{\beta})^2}{(1+\sqrt{2})^n}+\frac{(\widehat{\gamma})^2}{(1+\sqrt{2})^n}+\frac{(\widehat{\delta})^2}{(1+\sqrt{2})^n}\right]\\ &= \left[\frac{\widehat{\alpha}}{(1+\sqrt{2})^l}\right]^2+\left[\frac{\widehat{\beta}}{(1+\sqrt{2})^l}\right]^2+\left[\frac{\widehat{\gamma}}{(1+\sqrt{2})^l}\right]^2+\left[\frac{\widehat{\delta}}{(1+\sqrt{2})^l}\right]^2\end{aligned}$$

é uma soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$. ■

Lema 3.11 *Sejam $\pi, \nu \in \mathbb{Z}[\sqrt{2}]$ elementos primos totalmente positivos que estão acima de números primos p, q, respectivamente com $p, q \equiv -1 \pmod 8$. Então $\pi\nu$ é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$.*

Prova. Seja $\pi = a + b\sqrt{2}$. Então

$$N(\pi) = a^2 - 2b^2 = p \equiv -1 \pmod 8 .$$

Isto implica que $a^2 - 2b^2$ é ímpar. Logo, se $a^2 \equiv -1 \pmod 8$, então a é um número ímpar e $-2b \equiv -2 \pmod 8$ implica que $b \equiv 1 \pmod 4$. Logo, b também é um número ímpar. Assim,

$$2 \nmid a = 2l + 1 \text{ e } 2 \nmid b = 2r + 1.$$

Logo,

$$\begin{aligned}\pi &= 2l + 1 + (2r+1)\sqrt{2}\\ &= 1 + \sqrt{2} + 2(l + r\sqrt{2})\\ &= (1+\sqrt{2}) \pmod 2 \text{ em } \mathbb{Z}[\sqrt{2}].\end{aligned}$$

Portanto,

$$\pi \equiv (1+\sqrt{2}) \pmod 2 \text{ em } \mathbb{Z}[\sqrt{2}].$$

Da mesma forma, encontramos que

$$\nu \equiv (1+\sqrt{2}) \pmod 2 \text{ em } \mathbb{Z}[\sqrt{2}].$$

Pelo Lema 3.6, existem $\omega_1, \omega_2 \in U(\mathbb{Z}_C)$ e elementos $\lambda_1, \lambda_2 \in \mathbb{Z}_C$ tais que

$$\omega_1\pi = N(\lambda_1) \text{ e } \omega_2\nu = N(\lambda_2).$$

Consideremos

$$\omega_1\omega_2\pi\nu = N(\lambda_1\lambda_2).$$

Temos assim que $\omega_1\omega_2\pi\nu$ é a norma de um elemento de $\mathbb{Z}_C$, logo podemos escrever como soma de quatro quadrados de elementos de $\mathbb{Q}(\sqrt{2})$ e, portanto, é maior que zero. Agora, olhando para o seu conjugado, encontramos que $\overline{(\omega_1\omega_2\pi\nu)}$ também é uma soma de quatro quadrados e também maior que zero. Portanto, $\omega_1\omega_2\pi\nu$ é totalmente positivo. Mas como π e ν são totalmente positivos, devemos ter $\omega_1\omega_2$ totalmente positiva. Vimos no Lema anterior que a unidade também é totalmente positiva, aqui, fazendo a mesma análise, encontramos que $\omega_1\omega_2 = (1+\sqrt{2})^m$ deve ter sinal positivo e $m = 2r$. Assim,

$$\omega_1\omega_2 = (1+\sqrt{2})^m = [(1+\sqrt{2})^2]^r = [1+2+2\sqrt{2}]^r \equiv 1 \pmod 2.$$

Temos que

$$\begin{aligned} N(\lambda_1\lambda_2) &= \omega_1\omega_2\pi\nu = (1+\sqrt{2})^{2r}(1+\sqrt{2})(1+\sqrt{2}) \pmod 2 \\ &= (1+\sqrt{2})^{2r+2} \pmod 2 \\ &= [(1+\sqrt{2})^2]^{r+1} \pmod 2 \\ &= [1+2+2\sqrt{2}]^{r+1} \pmod 2 \\ &\equiv 1 \pmod 2 \text{ em } \mathbb{Z}[\sqrt{2}]. \end{aligned}$$

Pelo Lema 3.6 existe um elemento $\omega \in U(\mathbb{Z}_C)$ tal que $\lambda_1\lambda_2\omega \in \mathbb{Z}[\sqrt{2}][1,i,j,k]$. Seja

$$\lambda_1\lambda_2\omega = \alpha + \beta i + \gamma j + \delta k, \text{ com } \alpha,\beta,\gamma,\delta \in \mathbb{Z}[\sqrt{2}],$$

e como $m = 2r$ e

$$(1+\sqrt{2})^m\pi\nu = N(\lambda_1\lambda_2) = N(\lambda_1\lambda_2\omega) = \alpha^2+\beta^2+\gamma^2+\delta^2,$$

dividindo os dois lados desta igualdade por $(1+\sqrt{2})^m$, obtemos

$$\begin{aligned} \pi\nu &= \left[\frac{\alpha^2}{(1+\sqrt{2})^m} + \frac{\beta^2}{(1+\sqrt{2})^m} + \frac{\gamma^2}{(1+\sqrt{2})^m} + \frac{\delta^2}{(1+\sqrt{2})^m}\right] \\ &= \left[\frac{\alpha}{(1+\sqrt{2})^r}\right]^2 + \left[\frac{\beta}{(1+\sqrt{2})^r}\right]^2 + \left[\frac{\gamma}{(1+\sqrt{2})^r}\right]^2 + \left[\frac{\delta}{(1+\sqrt{2})^r}\right]^2, \end{aligned}$$

$$\begin{aligned} \pi\nu &= \left[\frac{\alpha^2}{(1+\sqrt{2})^m} + \frac{\beta^2}{(1+\sqrt{2})^m} + \frac{\gamma^2}{(1+\sqrt{2})^m} + \frac{\delta^2}{(1+\sqrt{2})^m}\right] \\ &= \left[\frac{\alpha}{(1+\sqrt{2})^r}\right]^2 + \left[\frac{\beta}{(1+\sqrt{2})^r}\right]^2 + \left[\frac{\gamma}{(1+\sqrt{2})^r}\right]^2 \\ &\quad + \left[\frac{\delta}{(1+\sqrt{2})^r}\right]^2, \end{aligned}$$

é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$. ■

3.2 Teorema de Cohn em Soma de Quatro Quadrados

Observação 3.12 *O termo radical de um elemento* $\pi \in \mathbb{Z}[\sqrt{2}]$ *que é soma de quatro quadrados deve ser par. Suponhamos que* $\pi = a + b\sqrt{2}$ *seja soma de quatro quadrados, ou seja,*

$$\pi = x^2 + y^2 + z^2 + w^2.$$

Consideremos $x = x_1 + x_2\sqrt{2}$, $y = y_1 + y_2\sqrt{2}$, $z = z_1 + z_2\sqrt{2}$ *e* $w = w_1 + w_2\sqrt{2}$. *Assim,*

$$\begin{aligned} a + b\sqrt{2} &= \pi = x^2 + y^2 + z^2 + w^2 \\ &= x_1^2 + 2x_1x_2\sqrt{2} + 2x_2^2 + y_1^2 + 2y_1y_2\sqrt{2} + 2y_2^2 \\ &\quad + z_1^2 + 2z_1z_2\sqrt{2} + 2z_2^2 + w_1^2 + 2w_1w_2\sqrt{2} + 2w_2^2 \\ &= x_1^2 + 2x_2^2 + y_1^2 + 2y_2^2 + z_1^2 + 2z_2^2 + w_1^2 + 2w_2^2 \\ &\quad + 2(x_1x_2 + y_1y_2 + z_1z_2 + w_1w_2)\sqrt{2}. \end{aligned}$$

Olhando apenas para o termo radical, temos que

$$b = 2(x_1x_2 + y_1y_2 + z_1z_2 + w_1w_2)$$

é um número par. Logo, π *só pode ser soma de quatro quadrados se* $2 \mid b$. *Observemos ainda que esta conta vale para* $\mathbb{Z}[\sqrt{d}]$ *com* $d \equiv 2$ *ou* $3 \pmod 4$.

Teorema 3.13 *Todo* $\pi = a + 2b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ *totalmente positivo é soma de quatro quadrados em* $\mathbb{Z}[\sqrt{2}]$.

Prova. Seja

$$\pi = a + 2b\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

Então

$$\pi \equiv 0 \text{ ou } 1 \pmod 2,$$

pois a pode ser um número par ou um número ímpar. Como $\mathbb{Z}[\sqrt{2}]$ é um domínio Euclidiano, podemos fatorar π de modo único e, sem perda de generalidade, podemos escolher estes primos todos totalmente positivos. Assim,

$$\pi = \omega(2 + \sqrt{2})^h \prod_{i=1}^{k} p_i \prod_{i=1}^{m} \gamma_i \prod_{i=1}^{n} \beta_i,$$

onde $\omega \in U(\mathbb{Z}[\sqrt{2}])$ e

$$2 + \sqrt{2} = \sqrt{2}(1 + \sqrt{2})$$

são os elementos que estão acima do número primo que ramifica, os p_i são os primos inertes em $\mathbb{Z}$, os elementos γ_i são os que estão acima do primo $q \equiv 1 \pmod 8$ e os elementos β_i são os que estão acima do primo $q \equiv -1 \pmod 8$. Como π é totalmente positivo e como escolhemos os primos todos totalmente positivos e, de modo análogo ao que foi feito na seção anterior, temos que ω também é totalmente positivo. Assim,

$$\omega = (1+\sqrt{2})^{2t}, \text{ para algum } t \in \mathbb{Z}.$$

Então

$$\pi = (3+2\sqrt{2})^t(2+\sqrt{2})^h \prod_{i=1}^{k} p_i \prod_{i=1}^{m} \gamma_i \prod_{i=1}^{n} \beta_i \pmod 2.$$

Como $\pi = a + 2b\sqrt{2} \equiv 0 \text{ ou } 1 \pmod 2$, temos que

$$\pi \equiv (\sqrt{2})^h(1+\sqrt{2})^n \pmod 2.$$

Logo,

$$(\sqrt{2})^h(1+\sqrt{2})^n \equiv 0 \text{ ou } 1 \pmod 2.$$

Temos, portanto, três casos a considerar:

1.^{o} **Caso**. Se $h = 0$, então n é par e, assim, os β_i formam pares, ou seja,

$$\beta_1\beta_2 \ldots \beta_{n-1}\beta_n,$$

e aplicando o Lema (3.11) a cada par obtemos que $\prod_{i=1}^{n} \beta_i$ é soma de quatro quadrados pela identidade de Lagrange. Então, pela identidade de Lagrange, π é soma de quatro quadrados em $\mathbb{Z}[\sqrt{2}]$.

2.^{o} **Caso**. Se $h = 1$ e $\begin{cases} 2 \mid n \\ 2 \nmid n \end{cases}$, então

$$\begin{aligned} \pi &\equiv \omega(2+\sqrt{2})^h \prod_{i=1}^{k} p_i \prod_{i=1}^{m} \gamma_i \prod_{i=1}^{n} \beta_i \pmod 2 \\ &\equiv \sqrt{2} \pmod 2. \end{aligned}$$

Mas

$$\pi \equiv 0 \text{ ou } 1 \pmod 2.$$

Então

$$\sqrt{2} \equiv 0 \text{ ou } 1 \pmod 2,$$

o que é um absurdo. Logo, este caso não existe, ou seja, $h > 1$. Portanto, $h \geq 2$.

3.^{o} **Caso**. Se $h \geq 2$, então

$$\begin{aligned}\pi &= \omega(2+\sqrt{2})^2(2+\sqrt{2})^{h-2}\prod_{i=1}^{k}p_i\prod_{i=1}^{m}\gamma_i\prod_{i=1}^{n}\beta_i \\ &= \omega 2(3+2\sqrt{2})(2+\sqrt{2})^{h-2}\prod_{i=1}^{k}p_i\prod_{i=1}^{m}\gamma_i\prod_{i=1}^{n}\beta_i.\end{aligned}$$

Pelo Lema (3.11) vimos que para cada elemento totalmente positivo β que está acima de um primo $q \equiv -1 \pmod 8$ existe um elemento $\omega \in U(\mathbb{Z}[\sqrt{2}])$ e um elemento $\lambda \in \mathbb{Z}_C$ tal que

$$\omega\beta = N(\lambda).$$

Temos que β é totalmente positivo e pelo Lema (3.8) temos que $N(\lambda)$ também é totalmente positiva, pois é soma de quatro quadrados. Logo, $\omega > 0$. Assim,

$$\overline{\omega}\overline{\beta} = \overline{N(\lambda)},$$

onde $\overline{N(\lambda)} > 0$, pois é soma de quatro quadrados, assim, $\overline{\omega} > 0$. Logo ω é totalmente positiva. Então podemos escrever

$$\omega = (1+\sqrt{2})^{2d}, \text{ para algum } d \in \mathbb{Z}.$$

Então

$$\beta = N((1+\sqrt{2})^{-d}\lambda),$$

e como $1+\sqrt{2} \in U(\mathbb{Z}[\sqrt{2}])$, temos que β é norma de algum elemento de $\mathbb{Z}_C$. Pela propriedade do produto da norma, temos que existe um $r \in \mathbb{Z}_C$ para o qual

$$N(r) = \prod_{i=1}^{n}\beta_i.$$

Além disso, podemos ver que

$$(2+\sqrt{2})^{h-2} = N((1+\rho_1)^{h-2}) \text{ e } \omega(3+2\sqrt{2}) = (1+\sqrt{2})^{2t+1}.$$

Assim,

$$\omega(3+2\sqrt{2})(2+\sqrt{2})^{h-2}\prod_{i=1}^{n}\beta_i = N((1+\sqrt{2})^{2t+1}(\rho_1+\rho_2)^{h-2}r).$$

Consideremos

$$s = (1+\sqrt{2})^{2t+1}(\rho_1+\rho_2)^{h-2}r, \text{ onde } s \in \mathbb{Z}_C.$$

Mas pode ser que $s \notin \mathbb{Z}[\sqrt{2}]\,[1,i,j,k]$. Se fosse o caso, a prova acabaria aqui, pois assim

$$s = x_1 + x_2 i + x_3 j + x_4 k, \ \text{ com } \ x_1, x_2, x_3, x_4 \in \mathbb{Z}[\sqrt{2}].$$

Logo,

$$N(s) = x_1^2 + x_2^2 + x_3^2 + x_4^2, \ \text{ com } \ x_1, x_2, x_3, x_4 \in \mathbb{Z}[\sqrt{2}].$$

Mas pelo Lema (3.5) temos, para todo $s \in \mathbb{Z}_C$, que existe um elemento $\omega \in U(\mathbb{Z}_C)$ tal que $\sqrt{2}s\omega$ é um elemento de $\mathbb{Z}[\sqrt{2}]\,[1,i,j,k]$. Assim,

$$\begin{aligned} N(\sqrt{2}s\omega) &= N(\sqrt{2})N(s)N(\omega) \\ &= 2\omega(3+2\sqrt{2})(2+\sqrt{2})^{h-2}\prod_{i=1}^{n}\beta_i. \end{aligned}$$

Mas considerando

$$\sqrt{2}s\omega = O_1 + O_2 i + O_3 j + O_4 k,$$

obtemos,

$$N(\sqrt{2}s\omega) = O_1^2 + O_2^2 + O_3^2 + O_4^2.$$

Então

$$2\omega(3+2\sqrt{2})(2+\sqrt{2})^{h-2}\prod_{i=1}^{n}\beta_i = O_1^2 + O_2^2 + O_3^2 + O_4^2$$

é soma de quatro quadrados de $\mathbb{Z}[\sqrt{2}]$. ■

Apêndice A

Resultados Básicos

Neste capítulo apresentaremos alguns resultados que serão necessários para o entendimento do exposto nos capítulos anteriores. O leitor interessado em mais detalhes pode consultar [2, 7, 8, 10].

A.1 Módulos

Nesta seção apresentaremos alguns resultados clássicos da teoria de módulos que serão necessários para a compreensão desta dissertação. Em toda esta dissertação a palavra anel significa, salvo menção explícita em contrário, anel comutativo com unidade.

Seja R um anel. Um *R-módulo* V é um grupo comutativo aditivo equipado com uma aplicação $R \times V \to V$,

$$R \times V \longrightarrow V, (r, \mathbf{v}) \longmapsto r\mathbf{v},$$

tal que as seguintes propriedades valem:

1. $r(s\mathbf{v}) = (rs)\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.

2. $(r + s)\mathbf{v} = r\mathbf{v} + s\mathbf{v}$, para quaisquer $r, s \in R$ e $\mathbf{v} \in V$.

3. $r(\mathbf{u} + \mathbf{v}) = r\mathbf{u} + r\mathbf{v}$, para qualquer $r \in R$ e $\mathbf{u}, \mathbf{v} \in V$.

4. $1\mathbf{v} = \mathbf{v}$, para todo $\mathbf{v} \in V$.

Note que, se R é um corpo, então um R-módulo é um espaço vetorial sobre R.

Um subconjunto não-vazio W de um R-módulo V é um *R-submódulo* de V se as seguintes condições são satisfeitas:

1. Para quaisquer $\mathbf{w}_1, \mathbf{w}_2 \in W$, têm-se $\mathbf{w}_1 - \mathbf{w}_2 \in W$.

2. Para quaisquer $r \in R$ e $\mathbf{w} \in W$, têm-se $r\mathbf{w} \in W$.

Sejam V um R-módulo e W um R-submódulo de V sobre R. Se $\mathbf{v}$ é um elemento arbitrário de V, escrevemos $[\mathbf{v}] = \mathbf{v} + W$ para representar o conjunto de todas as somas $\mathbf{v} + \mathbf{w}$, com $\mathbf{w} \in W$, isto é,

$$[\mathbf{v}] = \{\mathbf{v} + \mathbf{w} : \mathbf{w} \in W\}.$$

Estes conjuntos são chamados *classes laterais* de W em V. Estas classes particionam V em subconjuntos mutuamente disjuntos de mesma cardinalidade.

No teorema seguinte, utilizaremos as classes laterais de um R-submódulo W e de um R-módulo V, para definir um novo R-módulo, chamado *módulo quociente de V por W*, que será denotado por

$$\frac{V}{W}.$$

Teorema A.1 *Sejam V um R-módulo e W um R-submódulo de V. Então as classes laterais de W em V formam um R-módulo com as seguintes operações de adição e multiplicação por escalar*:

1. $[\mathbf{v}_1] + [\mathbf{v}_2] = [\mathbf{v}_1 + \mathbf{v}_2]$, *para quaisquer* $\mathbf{v}_1, \mathbf{v}_2 \in V$.

2. $r[\mathbf{v}] = [r\mathbf{v}]$, *para qualquer* $r \in R$ *e* $\mathbf{v} \in V$. ■

Sejam X um subconjunto de um R-módulo V e

$$\mathcal{F} = \{W : W \text{ é submódulo de } V \text{ e } X \subset W\}.$$

Então

$$\langle X \rangle = \bigcap_{W \in R} W$$

é o menor R-submódulo de V contendo X e será chamado de *R-submódulo gerado por X*. É claro que

$$\langle X \rangle = \left\{ \sum_{i=1}^{n} r_i \mathbf{x}_i : n \in N, \ \mathbf{x}_i \in X \text{ e } r_i \in R \right\}.$$

Se $X = \{\mathbf{v}\}$, isto é, X consiste de um único elemento, então,

$$\langle \mathbf{v} \rangle = \{r\mathbf{v} : r \in R\} = Rv$$

e $\langle \mathbf{v} \rangle$ será chamado de *R-submódulo cíclico gerado por* $\mathbf{v}$.

Quando existir um subconjunto finito $X = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de um R-módulo V tal que $V = \langle X \rangle$, dizemos que V é um *R-módulo finitamente gerado* e, neste caso,

$$V = \langle X \rangle = R\mathbf{x}_1 + \cdots + R\mathbf{x}_n.$$

Sejam U e V dois R-módulos. Uma função $T : U \to V$ é um *R-homomorfismo* se as seguintes condições são satisfeitas:

1. $T(\mathbf{u} + \mathbf{v}) = T(\mathbf{u}) + T(\mathbf{v})$, para todo $\mathbf{u}, \mathbf{v} \in U$.

2. $T(r\mathbf{u}) = rT(\mathbf{u})$, para todo $\mathbf{u} \in U$ e $r \in R$.

Um R-homomorfismo $T : U \longrightarrow V$ é um *R-isomorfismo* se T for bijetora. Denotaremos por

$$\mathrm{Hom}_R(U, V) = \{T : U \longrightarrow V : T \text{ é um } R\text{-homomorfismo}\}.$$

Em particular, quando $U = V$ temos que $\mathrm{Hom}_R(V, V) = \mathrm{End}_R(V)$.

Teorema A.2 (Propriedade Universal da Projeção) *Sejam V, W R-módulos e U um R-submódulo de V. Então para cada R-homomorfismo $T : V \to W$ com $U \subseteq \ker T$ existe um único R-homomorfismo $T_1 : \frac{V}{U} \to W$ tal que $T_1 \circ p = T$, e $p : V \to \frac{V}{U}$, onde p é um homomorfismo canônico $v \mapsto [v]$.* ■

Sejam V um R-módulo e X qualquer subconjunto não-vazio de V. Dizemos que V é um *R-módulo livre* sobre X se para cada elemento $v \in V$ existirem únicos elementos

$$x_1, x_2, \ldots, x_n \in X \text{ e } r_1, r_2, \ldots, r_n \in R$$

tais que

$$\mathbf{v} = r_1x_1 + r_2x_2 + \cdots + r_nx_n.$$

Dizemos que X é uma *R-base*.

Teorema A.3 *Para qualquer conjunto não-vazio X existe um R-módulo livre $R^{(X)}$ contendo X e $R^{(X)}$ satisfazendo a seguinte propriedade universal: se V é qualquer R-módulo e $\varphi : X \to V$ uma função. Então existe um único R-homomorfismo $\Phi : R^{(X)} \to V$ tal que $\Phi(x) = \varphi(x)$, para todo $x \in X$.*

Prova. Seja $R^{(X)}$ o conjunto de todas as funções $f : X \to R$ tais que $f(x) = 0$, para quase todo exceto um número finito de $x \in X$. Então $R^{(X)}$ equipado com a operação de adição

$$(f + g)(x) = f(x) + g(x), \ \forall \ x \in X \ \text{e} \ f, g \in R^{(X)},$$

e multiplicação por escalar

$$(rf)(x) = rf(x), \ \forall \ x \in X, \ r \in R \ \text{e} \ f \in R^{(X)}$$

é um R-módulo. Note que podemos identificar X com um subconjunto de $R^{(X)}$ por $x \to e_x(y)$, onde

$$e_x(y) = \begin{cases} 1 & \text{se } x = y \\ 0 & \text{se } x \neq y \end{cases}, \ \forall \ x, y \in X.$$

Assim, cada elemento de $f \in R^{(X)}$ tem uma única expressão como uma soma formal

$$f = \sum_{i=1}^{n} f(x_i)e_{x_i} = \sum_{i=1}^{n} r_i x.$$

Suponhamos que $\varphi : X \to V$, onde V é qualquer R-módulo. Definimos $\Phi : R^{(X)} \to V$ por

$$\Phi\left(\sum_{i=1}^{n} r_i x\right) = \sum_{i=1}^{n} r_i \varphi(x_i).$$

Pela unicidade da soma é claro que Φ está bem definida e é um R-homomorfismo. Por definição $\Phi(x) = \varphi(x)$, para todo $x \in X$. Finalmente, seja $\Psi : R^{(X)} \to V$ qualquer R-homomorfismo tal que $\Psi(x) = \varphi(x)$, para todo $x \in X$. Então

$$\Phi(x) = \varphi(x) = \Psi(x), \ \forall \ x \in X.$$

Como $R^{(X)}$ é gerado por X temos que $\Phi = \Psi$. Portanto, Φ é único. ■

Teorema A.4 *Sejam V, W R-módulos e $p : V \to W$ um R-homomorfismo sobrejetor. Então para cada R-homomorfismo $T : U \to W$ com U um R-módulo livre existe um único R-homomorfismo $S : U \to V$ tal que $T = p \circ S$.*

Prova. Como $U = R^{(X)}$ para algum conjunto não-vazio X de U e p é sobrejetor temos que para cada $x \in X$ existe algum $\mathbf{w}_x \in V$ tal que $p(\mathbf{w}_x) = T(e_x)$. Sendo $U = R^{(X)}$ um R-módulo livre temos que existe um único R-homomorfismo $S : U \to V$ tal que $S(e_x) = w_x$. Portanto,

$$(p \circ S)(e_x) = p(S(e_x)) = p(w_x) = T(e_x),$$

Concluímos daí que, $T = p \circ S$. ■

Teorema A.5 *Sejam R um domínio principal e V um R-módulo livre de posto n, onde o posto é visto como a cardinalidade da base do R-módulo. Então todo R-submódulo W de V é livre com posto $m \leq n$.* ■

Seja V um R-módulo. Para qualquer $X \subseteq V$, definimos o *anulador* de X em R como

$$\mathrm{Ann}_R(X) = \{r \in R : rx = 0 \ \forall \ x \in X\}.$$

É fácil verificar que $\mathrm{Ann}_R(X)$ é um ideal de R.

Sejam U, V e W R-módulos. Uma função $B : U \times V \to W$ é R-bilinear se as seguintes condições são satisfeitas:

1. $B(ru_1 + u_2, v) = rB(u_1, v) + B(u_2, v)$, para todo $u_1, u_2 \in U$, $v \in V$ e $r \in R$.

2. $B(u, sv_1 + v_2) = sB(u, v_1) + B(u, v_2)$, para todo $u \in U$, $v_1, v_2 \in V$ e $s \in R$.

   Vamos denotar o conjunto de todas as transformações R-bilineares de $U \times V$ em W por

   $$\mathcal{L}^2(U, V; W).$$

Sejam V um F-espaço vetorial e $\mathbf{v}_1, \ldots, \mathbf{v}_n$ vetores de V. Então $[B(\mathbf{v}_i, \mathbf{v}_j)]$ é uma matriz $n \times n$ sobre F. O *discriminante* de $\mathbf{v}_1, \ldots, \mathbf{v}_n$ com relação a B é definido por

$$\det\left([B(\mathbf{v}_i, \mathbf{v}_j)]\right)$$

e será denotado por

$$\Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

Proposição A.6 *Sejam V um F-espaço vetorial e $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ uma F-base qualquer para V. Sejam $\mathbf{w}_1, \ldots, \mathbf{w}_n$ vetores quaisquer de V. Se*

$$\mathbf{w}_i = \sum_{j=1}^{n} a_{ij}\mathbf{v}_j, i = 1, \ldots, n,$$

com $a_{ij} \in F$, então

$$\Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = (\det \mathbf{A})^2 \Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n),$$

onde $\mathbf{A} = [a_{ij}]$.

Prova. Seja

$$\mathbf{w}_k = \sum_{l=1}^{n} a_{kl}\mathbf{v}_l, k = 1, \ldots, n.$$

Então é fácil verificar que

$$B(\mathbf{w}_i, \mathbf{w}_k) = \sum_{l=1}^{n} \left(\sum_{j=1}^{n} a_{ij} B(\mathbf{v}_j, \mathbf{v}_l) \right) a_{kl}.$$

Portanto,

$$[B(\mathbf{w}_i, \mathbf{w}_k)] = \mathbf{A}[B(\mathbf{v}_j, \mathbf{v}_l)]\mathbf{A}^t \text{ e } \Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = (\det \mathbf{A})^2 \Delta(\mathbf{v}_1, \ldots, \mathbf{v}_n).$$

■

Corolário A.7 *Sejam V um F-espaço vetorial e $\mathbf{w}_1, \ldots, \mathbf{w}_n$ vetores quaisquer de V. Se $\mathbf{w}_1, \ldots, \mathbf{w}_n$ são linearmente dependentes, então*

$$\Delta(\mathbf{w}_1, \ldots, \mathbf{w}_n) = 0.$$

■

A.2 Extensões de Corpos

Sejam K e F dois corpos. Dizemos que F é uma *extensão* de K se $K \subseteq F$ e será denotada por $K \subseteq F$ ou F/K.

Sejam F uma extensão de K e $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$. Então

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

denotará o menor subcorpo de F contendo $\alpha_1, \alpha_2, \ldots, \alpha_n$ e K. Uma extensão F de K é chamada *finitamente gerada sobre* K se existir $\alpha_1, \alpha_2, \ldots, \alpha_n \in F$ tais que

$$F = K(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Se existir $\alpha \in F$ tal que $F = K(\alpha)$, dizemos que F é uma *extensão simples* de K e α é chamado um *elemento primitivo* de F sobre K.

Sejam F uma extensão de K e α um elemento de F. Dizemos que α é *algébrico* sobre K se existirem $a_0, a_1, \ldots, a_n \in K$, com $a_n \neq 0$, tais que

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

isto é, existe um polinômio não-nulo $f \in K[x]$ tal que $f(\alpha) = 0$. Caso contrário, α é *transcendente* sobre K. Note que todo $\alpha \in K$ é algébrico sobre K, pois α é raiz do polinômio $p = x - \alpha \in K[x]$. Se todo elemento de uma extensão $K \subseteq F$ for algébrico sobre K, dizemos que F é uma *extensão algébrica*.

Proposição A.8 *Sejam F uma extensão de K e α um elemento de F. Então a função $\phi : K[x] \to F$ definida por $\phi(f) = f(\alpha)$ é um homomorfismo de anéis tal que*:

1. $\operatorname{Im}\phi = K[\alpha]$ *e* $K \subseteq K[\alpha] \subseteq F$.

2. α *é transcendente sobre* K *se, e somente se,* $\ker\phi = \{0\}$.

3. α *é algébrico sobre* K *se, e somente se,* $\ker\phi \neq \{0\}$.

4. $\frac{K[x]}{\ker\phi} \simeq K[\alpha]$. ■

Sejam F uma extensão de K e $\alpha \in F$ algébrico sobre K. Como

$$\frac{K[x]}{\langle p\rangle} \simeq K[\alpha] \subset F.$$

Segue-se que $\frac{K[x]}{\langle p\rangle}$ é um domínio. Logo, $\langle p\rangle$ é um ideal primo primo. Sendo $K[x]$ um domínio de fatoração, isto implica que $\langle p\rangle$ é um ideal maximal. Portanto, p é irredutível, e denotamos $p = \operatorname{irr}(\alpha, K)$. Assim, $K[\alpha]$ é um corpo e $K[\alpha] = K(\alpha)$.

Seja $K \subseteq F$ uma extensão. Então F com as operações de adição

$$\begin{array}{rccc} + : & F \times F & \to & F \\ & (a,b) & \mapsto & a+b \end{array}$$

e multiplicação por escalar

$$\begin{array}{rccc} \cdot : & K \times F & \to & F \\ & (\lambda, a) & \mapsto & \lambda a \end{array},$$

é um K-espaço vetorial. O *grau* de uma extensão $K \subseteq F$, denotado por $[F : K]$, é a dimensão de F visto como K-espaço vetorial. A extensão será chamada *finita* se $[F : K] = n < \infty$. Caso contrário, a extensão será chamada *infinita*.

Teorema A.9 *Sejam F uma extensão de K e α um elemento de F. Então α é algébrico sobre K se, e somente se, $K(\alpha)$ é uma extensão finita de K. Neste caso, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base para $K(\alpha)$ e $[K(\alpha) : K] = n = \partial(p)$, onde $p = \operatorname{irr}(\alpha, K)$.* ■

Proposição A.10 *Sejam $K \subseteq F \subseteq E$ corpos tais que $[E : F]$ e $[F : K]$ sejam finitos. Então $[E : K]$ é finito e*

$$[E : K] = [E : F]\,[F : K]$$

■

Sejam K um corpo e $f \in K[x]$. Um *corpo de decomposição* de f sobre K é uma extensão de F sobre K tal que

1. f se fatora em F;
2. F é minimal com respeito à condição 1., isto é, se f se fatora em Z com $K \subseteq Z \subseteq F$, então $Z = F$.

Teorema A.11 *Seja K um corpo. Então qualquer $f \in K[x]$ possui um corpo de decomposição.* ■

Seja K um corpo. Dizemos que K é *algebricamente fechado* se qualquer polinômio não constante sobre K pode ser decomposto em fatores lineares sobre K.

Proposição A.12 *Seja K um corpo. Então as seguintes condições são equivalentes*:

1. *K é algebricamente fechado*;
2. *Qualquer polinômio não constante $f \in K[x]$ tem uma raiz em K*;
3. *Se F é uma extensão algébrica de K, então $F = K$.* ■

Seja K um corpo. Um *fecho algébrico* de K é uma extensão algébrica F de K tal que as seguintes condições são satisfeitas:

1. F é algebricamente fechado.
2. F é minimal com respeito à condição 1., isto é, se Z é um corpo algebricamente fechado tal que $K \subseteq Z \subseteq F$, então $Z = F$.

Vamos denotar o fecho algébrico de K por $\overline{K}$. Neste caso, $\overline{K}$ é uma extensão algébrica de K.

Seja $K \subseteq F$ uma extensão. Dizemos que F é *normal* se F é um corpo de decomposição de alguma família $\mathcal{F} \subseteq K[x]$ de polinômios sobre K.

Proposição A.13 *Sejam $F = K[\alpha]$ com α algébrico, $p = \mathrm{irr}(\alpha, K) \in K[x]$ e N uma extensão normal de K contendo α. Se $\beta \in N$, então as seguintes condições são equivalentes*:

1. *$\beta \in N$ é uma raiz de p.*

2. *$p = \mathrm{irr}(\alpha, K) = \mathrm{irr}(\beta, K)$.*

3. *Existe um único K-isomorfismo $\sigma : K(\alpha) \to K(\beta)$, com $\sigma(\alpha) = \beta$.*

4. *Existe um K-automorfismo $\varphi : N \to N$, com $\varphi(\alpha) = \beta$.* ■

Se pelo menos uma (e portanto todas) das quatro condições da Proposição A.13 for satisfeita, dizemos que β é um *conjugado de α sobre K*. Conseqüentemente, o número de K-imersões de $K(\alpha)$ em N é menor ou igual ao número de raízes de p, isto é,

$$\mathrm{Hom}_K(F, N) \leq \partial(p) = [K[\alpha] : K].$$

Sejam $p \in K[x]$ um polinômio irredutível sobre K e L um corpo de decomposição para p. Dizemos que p é *separável* sobre K se todas as raízes de p em L são simples ou, equivalentemente,

$$\mathrm{mdc}(p, p') = 1.$$

Seja $f \in K[x]$ um polinômio qualquer. Dizemos que f é *separável* sobre K se cada um de seus fatores irredutíveis é separável sobre K.

Sejam F/K uma extensão e $\alpha \in F$. Dizemos que α é *separável* sobre K se α é algébrico sobre K e $\mathrm{irr}(\alpha, K)$ é separável sobre K. Dizemos que F/K é uma *extensão separável* se cada elemento de F for separável sobre K.

Teorema A.14 *Seja F uma extensão separável de K com $[F : K] < \infty$. Então existe $\alpha \in F$ tal que $F = K[\alpha]$.* ■

A.3 Traços e Normas

Nesta seção todas as extensões de K, salvo menção explícita em contrário, são separáveis.

Sejam F uma extensão finita de K com $[F : K] = n$ e $\alpha \in F$. Então a função $\phi_\alpha : F \to F$ definida por $\phi_\alpha(\beta) = \alpha\beta$ é claramente uma transformação K-linear sobre

F. Logo, a função $\varphi : F \to \mathrm{End}_K F = \mathrm{Hom}_K(F,F)$ definida por $\varphi(\alpha) = \phi_\alpha$ é um homomorfismo de anéis injetor. Portanto, podemos identificar F com um subcorpo do anel $\mathrm{End}_K F$. Se

$$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

é uma K-base para F e

$$\phi_\alpha(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i, j = 1, \ldots, n,$$

então

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A})$$

é o *polinômio característico* de α sobre K, onde $\mathbf{A} = [a_{ij}]$ é a matriz $n \times n$ da transformação linear ϕ_α em relação à K-base $\mathcal{B}$.

Teorema A.15 *Sejam F uma extensão de K com $[F:K] = n$ e $\alpha \in F$. Se $p = \mathrm{irr}(\alpha, K)$, então $f_\alpha = p^k$, onde $k = [F : K[\alpha]]$. Além disso, $f_\alpha = p$ se, e somente se, $F = K[\alpha]$.*

Prova. Seja

$$p(x) = \mathrm{irr}(\alpha, K) = c_0 + c_1 x + \cdots + c_{m-1}x^{m-1} + x^m.$$

Então $\{1, \alpha, \ldots, \alpha^{m-1}\}$ é uma K-base para $K[\alpha]$. Se $\{\beta_0, \ldots, \beta_{k-1}\}$ é uma $K[\alpha]$-base para F, então

$$\{\alpha^i\beta_j : 0 \leq i \leq m-1 \text{ e } 0 \leq j \leq k-1\}$$

é uma K-base para F. Logo, a matriz de ϕ_α nesta base é da forma

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_0 & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{A}_1 & \cdots & \mathbf{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{A}_{k-1} \end{pmatrix},$$

onde

$$\mathbf{A}_j = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -c_{m-2} \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}.$$

Portanto,

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}) = \prod_{j=0}^{k-1} \det(x\mathbf{I} - \mathbf{A}_j) = p(x)^k.$$

Finalmente, se $f_\alpha = p$, então

$$[K[\alpha] : K] = n = [F : K].$$

Logo, $F = K[\alpha]$. Reciprocamente, se $F = K[\alpha]$, então $\partial p = n$ e $f_\alpha = p$. ■

Seja $\mathbf{A}$ a matriz da transformação linear ϕ_α em relação à alguma K-base. O *traço* e a *norma* de α são definidos por

$$\operatorname{tr}(\alpha) = \operatorname{tr}(\mathbf{A}) \text{ e } N(\alpha) = \det(\mathbf{A}).$$

Proposição A.16 *Seja F uma extensão de K com $[F : K] = n$.*

1. $\operatorname{tr}(a\alpha + b\beta) = a\operatorname{tr}(\alpha) + b\operatorname{tr}(\beta)$, *para todo $a, b \in K$ e $\alpha, \beta \in F$.*

2. $\operatorname{tr}(a) = na$, *para todo $a \in K$.*

3. $N(\alpha\beta) = N(\alpha)N(\beta)$, *para todo $\alpha, \beta \in F$.*

4. $N(a) = a^n$, *para todo $a \in K$.* ■

Suponhamos que

$$f_\alpha(x) = (x - \alpha_0) \cdots (x - \alpha_{n-1})$$

em $\overline{K}$. Então

$$\operatorname{tr}(\alpha) = \sum_{j=0}^{n-1} \alpha_j \text{ e } N(\alpha) = \prod_{j=0}^{n-1} \alpha_j.$$

De fato, se

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

então

$$a_{n-1} = -\operatorname{tr}(\mathbf{A}) \text{ e } a_0 = (-1)^n \det(\mathbf{A}).$$

Por outro lado, é fácil verificar que

$$\sum_{j=0}^{n-1} \alpha_j = -a_{n-1} \text{ e } \prod_{j=0}^{n-1} \alpha_j = (-1)^n a_0.$$

Portanto, $\operatorname{tr}(\alpha) \in K$ e $N(\alpha) \in K$.

Corolário A.17 *Seja F uma extensão de K com $[F : K] = n$. Se $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, são as K-imersões de$F$ em $\overline{K}$, então para todo $\alpha \in F$ temos que*

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

Além disso,

$$\mathrm{tr}(g(\alpha)) = \sum_{i=1}^{n} g(\alpha_i) \ \ e \ \ N(g(\alpha)) = \prod_{i=1}^{n} g(\alpha_i),$$

para todo $\alpha \in F$ e $g \in K[x]$, onde $\alpha_i = \sigma_i(\alpha)$, $i = 1, \ldots, n$. ■

A função $B : F \times F \to K$ definida por $B(\alpha, \beta) = \mathrm{tr}(\alpha\beta)$ é claramente uma forma K-bilinear simétrica. Logo, por definição, o discriminante de uma K-base

$$\mathcal{B} = \{1, \theta, \ldots, \theta^{n-1}\}$$

para F é

$$\Delta(\mathcal{B}) = \det(\mathrm{tr}(\theta^{i+j})).$$

Se $\mathcal{B}' = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ é uma outra base de F tal que

$$\alpha_i = \sum_{j=0}^{n-1} a_{ij}\theta^j,$$

onde $\mathbf{B} = [a_{ij}]$ é a matriz mudança de base, então pela Proposição A.6 temos que

$$\Delta(\mathcal{B}') = (\det \mathbf{B})^2 \Delta(\mathcal{B}).$$

Proposição A.18 *Seja F uma extensão de K com $[F : K] = n$.*

1. *Se $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, são as K-imersões de F,onde F é algebricamente fechado, então*

   $$\Delta(\mathcal{B}) = (\det(\sigma_i(\alpha_j)))^2$$

   onde

   $$\mathcal{B} = \{\alpha_1, \ldots, \alpha_n\}$$

   é uma K-base para F.

2. *Se $F = K(\alpha)$ e $p = \mathrm{irr}(\alpha, K) \in K[x]$, então*

   $$\Delta(\mathcal{B}') = (-1)^{\frac{n(n-1)}{2}} N(p'(\alpha)) = \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (\sigma_j(\alpha) - \sigma_i(\alpha))^2,$$

onde

$$\mathcal{B}' = \{1, \alpha, \ldots, \alpha^{n-1}\}$$

é uma K-base para F.

Prova. Vamos provar apenas o item 1. Sejam

$$\mathbf{A} = [a_{ij}] \text{ e } \mathbf{A}^t = [b_{ij}]$$

onde $a_{ij} = \sigma_i(\alpha_j)$ e $b_{ij} = a_{ji}$. Então

$$\mathbf{A}^t\mathbf{A} = [c_{ij}],$$

onde

$$c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj} = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \operatorname{tr}(\alpha_i\alpha_j).$$

Logo,

$$\Delta(\mathcal{B}') = \det(\operatorname{tr}(\alpha_i\alpha_j)) = \det(\mathbf{A}^t\mathbf{A}) = (\det(\mathbf{A}))^2.$$

■

Teorema A.19 *Seja F uma extensão finita de K. Então as seguintes condições são equivalentes*:

1. $\operatorname{tr} : F \to K$ *é sobrejetora.*

2. *Existe $\alpha \in F^*$ tal que $\operatorname{tr}(\alpha) \neq 0$.*

3. *A forma bilinear $B : F \times F \to K$ definida por $B((\alpha, \beta)) = \operatorname{tr}(\alpha\beta)$ é não-degenerada.*

Prova. É claro que (2 $\Rightarrow$ 1). Para provar que (1. $\Rightarrow$ 2.). Suponhamos que exista $\alpha \in F$ com $\operatorname{tr}(\alpha) = b \neq 0$. Logo,

$$\operatorname{tr}(cb^{-1}\alpha) = cb^{-1}\operatorname{tr}(\alpha) = cb^{-1}b = c, \forall c \in K.$$

Portanto, tr é sobrejetora.

(1. $\Rightarrow$ 3.) Suponhamos que tr seja sobrejetora. Então existe $\alpha \in F^*$ tal que $\operatorname{tr}(\alpha) \neq 0$. Dado $\beta \in F^*$, existe $\alpha\beta^{-1} \in F$ tal que

$$B(\alpha\beta^{-1}, \beta) = \operatorname{tr}(\alpha\beta^{-1}\beta) = \operatorname{tr}(\alpha) \neq 0.$$

Portanto, B é não degenerada.

(3. $\Rightarrow$ 1.) Segue da definição. ■

A.4 Inteiros Algébricos

Sejam $R \subseteq S$ uma extensão de anéis e α um elemento de S. Dizemos que α é um *inteiro algébrico* sobre R se existir $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

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

Se todo elemento de uma extensão $R \subseteq S$ for inteiro, dizemos que S é uma *extensão inteira* de R.

Teorema A.20 *Sejam $R \subseteq S$ uma extensão de anéis e α um elemento de S. Então as seguintes condições são equivalentes*:

1. *α é um inteiro sobre R*;
2. *$R[\alpha]$ é um R-módulo finitamente gerado*;
3. *Existe um anel Z com $R[\alpha] \subseteq Z \subseteq S$ tal que Z é um R-módulo finitamente gerado*;
4. *Existe um $R[\alpha]$-módulo V, o qual é um R-módulo finitamente gerado e cujo*

$$\mathrm{Ann}_{R[\alpha]}(V) = \{0\}.$$

■

Lema A.21 *Sejam $R \subseteq S \subseteq T$ anéis.*

1. *Se S é um R-módulo finitamente gerado e T é um S-módulo finitamente gerado, então T é um R-módulo finitamente gerado.*
2. *Se $\mathrm{Ann}_R(S) = \{0\}$ e S é um R-módulo finitamente gerado, então o único ideal I em R com $IS = S$ é $I = R$.*

Prova. 1. Se

$$S = R\alpha_1 \oplus \cdots \oplus R\alpha_m \text{ e } T = S\beta_1 \oplus \cdots \oplus S\beta_n,$$

então

$$T = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} R\alpha_i \right) \beta_j = \sum_{i=1}^{m} \sum_{j=1}^{n} R\alpha_i\beta_j.$$

Portanto, T é um R-módulo finitamente gerado.

2. Suponhamos que

$$S = R\alpha_1 \oplus \cdots \oplus R\alpha_n.$$

Como $\alpha_i \in S$ e

$$S = IS = I\alpha_1 \oplus \cdots \oplus I\alpha_n$$

temos que existem $a_{ij} \in I$ tais que

$$\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j, \;\; j = 1, \ldots, n.$$

Ou na forma matricial

$$(\mathbf{A} - \mathbf{I}_n)\mathbf{X} = \mathbf{O},$$

onde

$$\mathbf{A} - \mathbf{I}_n = \begin{bmatrix} a_{11} - 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - 1 \end{bmatrix} \text{ e } \mathbf{X} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}.$$

Como $\det(\mathbf{A} - \mathbf{I}_n)\mathbf{I}_n = \text{adj}(\mathbf{A} - \mathbf{I}_n)(\mathbf{A} - \mathbf{I}_n)$ temos que $\det(\mathbf{A} - \mathbf{I}_n)\mathbf{X} = \mathbf{0}$. Assim,

$$\det(\mathbf{A} - \mathbf{I}_n)\alpha_i = 0 \;\; i = 1, \ldots, n,$$

isto é, $\det(\mathbf{A} - \mathbf{I}_n) \in \text{Ann}(S) = \{0\}$. Por outro lado, a expansão do determinante mostra que $\det(\mathbf{A} - \mathbf{I}_n) = (-1)^n + x$, com $x \in I$, pois $a_{ij} \in I$. Portanto, $1 \in I$ e $I = R$. ■

Seja $R \subseteq S$ uma extensão de anéis. O *fecho inteiro* de R em S é definido como

$$R_S = \{\alpha \in S : \alpha \text{ é inteiro sobre } R\}.$$

Dizemos que R é *integralmente fechado* em S se $R_S = R$.

Teorema A.22 *Sejam $R \subseteq S \subseteq T$ extensões de anéis.*

1. *Se S é um R-módulo finitamente gerado, então S é uma extensão inteira de R.*
2. *Se $\alpha_1, \ldots, \alpha_n \in S$ são inteiros sobre R, então $R[\alpha_1, \ldots, \alpha_n]$ é um R-módulo finitamente gerado.*
3. *R_S é um anel com $R \subseteq R_S \subseteq S$.*
4. *Se $S = R_T$, então S é integralmente fechado em T.* ■

Corolário A.23 *Sejam R um domínio de fatoração única e K seu corpo quociente. Então $R_K = R$.* ■

Proposição A.24 *Seja $R \subseteq S$ uma extensão de domínios tal que S é uma extensão inteira de R. Então S é um corpo se, e somente se, R também o é.*

Prova. Suponhamos que S seja um corpo. Então para cada $\alpha \in R^*$, obtemos $\alpha^{-1} \in S$, pois S é um corpo. Logo, por hipótese, existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

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

Multiplicando esta equação por α^{m-1}, obtemos

$$\alpha^{-1} = -(a_{m-1} + \cdots + a_1\alpha^{m-2} + a_0\alpha^{m-1}) \in R.$$

Portanto, R é um corpo. Reciprocamente, suponhamos que R seja um corpo. Para cada $\alpha \in S^*$, existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

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

onde n é mínimo. Então $a_0 \neq 0$ e $a_0^{-1} \in R$. Assim,

$$\alpha(a_1 + \cdots + a_{n-1}\alpha^{n-2} + \alpha^{n-1})(-a_0^{-1}) = 1,$$

isto é, α é invertível. Portanto, S é um corpo. ■

Corolário A.25 *Seja $R \subseteq S$ uma extensão de domínios tal que S é uma extensão inteira sobre R.*

1. *Para qualquer ideal I não-nulo de S, $I \cap R$ é um ideal não-nulo de R.*
2. *$U(S) \cap R = U(R)$.*
3. *Um ideal M de S é maximal se, e somente se, $N = M \cap R$ é um ideal maximal de R.* ■

Proposição A.26 *Sejam R um dominio, K seu corpo quociente com $R_K = R$, F uma extensão finita de K e $S = R_F$.*

1. *Se $\alpha \in S$, então $\sigma_i(\alpha)$ são inteiros sobre R, onde $\sigma_i : F \longrightarrow \overline{K}$, $i = 1, \ldots, n$, são as K-imersões de F em $\overline{K}$.*

2. *Se $\alpha \in S$, então $\mathrm{tr}(\alpha), N(\alpha) \in R$.*

3. *$\alpha \in U(S)$ se, somente se, $N(\alpha) \in U(R)$.*

4. *Se $\alpha \in R$ é tal que $N(\alpha)$ é irredutível em R, então α é irredutível em S.*

5. *Qualquer elemento de F pode ser escrito na forma $\frac{c}{a}$, onde $c \in S$ e $a \in R$. Em particular, F é o corpo quociente de S, ou seja, $F = R^{-1}S$.*

Prova. 1. Seja $\alpha \in S$. Então existem $a_0, a_1, \ldots, a_{n-1} \in R$ tais que

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

Logo

$$0 = \sigma_i(0) = \sigma_i\left(\sum_{i=0}^{n} a_i\alpha^i\right) = \sum_{i=0}^{n} a_i\sigma_i(\alpha^i).$$

Portanto, $\sigma_i(\alpha)$ inteiro sobre R.

2. É claro que o $\mathrm{tr}(\alpha) \in K$ e $N(\alpha) \in K$. Por outro lado, como $\sigma_i(\alpha)$ são inteiros sobre R temos, pelo Corolário A.17, que $\mathrm{tr}(\alpha)$ e $N(\alpha)$ são inteiros sobre R. Logo, $\mathrm{tr}(\alpha), N(\alpha) \in R_K = R$.

3. Suponhamos que $\alpha \in U(S)$. Então existe $\beta \in S$ tal que $\alpha\beta = 1$. Logo,

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Portanto, $N(\alpha) \in U(R)$. Reciprocamente, se $N(\alpha) \in U(R)$, então existe $a \in R$ tal que $aN(\alpha) = 1$. Logo,

$$1 = aN(\alpha) = a\prod_{j=1}^{n} \sigma_j(\alpha).$$

Como $\sigma_j = id$, para algum $j = 1, \ldots, n$, temos que $\alpha \in U(S)$, onde

$$\alpha^{-1} = (a \prod_{i=1, i\neq j}^{n} \sigma_i(\alpha)).$$

4. Segue da definição de elemento irredutível e do item 3.

5. Dado $\alpha \in F$. Como α é algébrico sobre K temos que existem $r_0, r_1, \ldots, r_{n-1} \in K$ tais que

$$r_0 + r_1\alpha + \cdots + r_{n-1}\alpha^{n-1} + \alpha^n = 0.$$

Fazendo

$$r_i = \frac{a_i}{b_i} \text{ e } \beta = b_0 b_1 \cdots b_{n-1} \in R,$$

obtemos

$$c_0 + c_1(\alpha\beta) + \cdots + c_{n-1}(\alpha\beta)^{n-1} + (\alpha\beta)^n = 0.$$

Assim, $\beta\alpha \in S = R_F$. Portanto, existe $c \in S$ tal que $\alpha = \frac{c}{\beta}$. ■

Proposição A.27 *Sejam R um dominio, K seu corpo quociente, F uma extensão de K e $S = R_F$.*

1. *Se $\alpha \in K \cap S$, então existe $c \in R^*$ tal que $c\alpha^n \in R$, para todo $n \in \mathbb{N}$.*

2. *Se $R_K = R$, então $K \cap S = R$.*

3. *Se $R_K = R$ e $\alpha \in S$, então $p = \text{irr}(\alpha, K) \in K[x]$ tem coeficientes em R.*

Prova. 1. Como $\alpha \in K \cap S$ temos que $\alpha = \frac{r}{s}$, com $r, s \in R$ e $\text{mdc}(r, s) = 1$, e existem $a_0, a_1, \ldots, a_{k-1} \in R$ tais que

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

Logo,

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + r^n = 0 \Rightarrow s \mid 1.$$

Assim, existe $t = s^{-1} \in R^*$ tal que $t\alpha = r \in R$. Portanto, indutivamente, obtemos $c\alpha^n \in R$, para todo $n \in \mathbb{N}$.

2. É claro que $R \subseteq K \cap S$. Mas por 1. $K \cap S \subseteq R$. Portanto, $K \cap S = R$.

3. Suponhamos que $\alpha \in S$ e $p = \text{irr}(\alpha, K)$. Então, pelo item 1.da Proposição A.26, os conjugados $\sigma_i(\alpha)$ de α são inteiros sobre $R = R_K$. Como os coeficientes de p são polinômios simétricos elementares das raízes temos, pelo item 4. do Teorema A.22, que eles são inteiros sobre R. Por outro lado, esses coeficientes estão K e $R_K = R$ implica que eles estão em R. ■

A.5 Reticulados

Seja $\mathbb{L}$ um $\mathbb{R}$-espaço de dimensão n. Tomando $\mathbf{e}_1, \ldots, \mathbf{e}_n$ uma base em $\mathbb{L}$ e definindo para os vetores $\mathbf{x} = x_1\mathbf{e}_1 + \cdots + x_n\mathbf{e}_n$ e $\mathbf{y} = y_1\mathbf{e}_1 + \cdots + y_n\mathbf{e}_n$, o produto escalar

$$(\mathbf{x}, \mathbf{y}) = \mathbf{x}\mathbf{y}^t = x_1y_1 + \cdots + x_ny_n,$$

e o comprimento

$$\|x\| = \sqrt{(x,x)} = \sqrt{x_1^2 + \cdots + x_n^2}$$

do vetor $\mathbf{x} \in \mathbb{L}$. Seja B_ρ a bola de raio ρ centrada na origem, ou seja,

$$B_\rho = \{\mathbf{x} \in \mathbb{L} : \|x\| \leq \rho\}.$$

Dados $\mathbf{z}_1, \ldots, \mathbf{z}_m \in \mathbb{L}$, consideremos os conjuntos

$$\Lambda = \mathbb{Z}\mathbf{z}_1 + \cdots + \mathbb{Z}\mathbf{z}_m = \left\{ \sum_{i=1}^{m} a_i z_i : a_1, \ldots, a_m \in \mathbb{Z} \right\}$$

e

$$T_{\mathbf{z}} = \{\sum_{i=1}^{m} \rho_i \mathbf{z}_i : 0 \leq \rho_i < 1, i = 1, \ldots, m\}.$$

Assim, Λ é um *reticulado* de $\mathbb{L}$ quando $\mathbf{z}_1, \ldots, \mathbf{z}_m$ forem linearmente independentes em $\mathbb{R}$ e $T_{\mathbf{z}}$ a *região fundamental*, neste caso, temos que $m \leq n$.

Exemplo A.28 *O conjunto de vetores*

$$\Lambda = \{a(1,0) + b(0,1) : a, b \in \mathbb{Z}\}$$

é um reticulado de dimensão 2 *em* $\mathbb{R}^2$ *com* $T_{\mathbf{z}} = [0,1) \times [0,1)$.

Um subconjunto C de $\mathbb{L}$ é *limitado*, se $C \subseteq B_\rho$ para algum $\rho > 0$. E um subconjunto D é *discreto*, se $D \cap B_\rho$ for finito, para todo $\rho \in \mathbb{R}$ com $\rho > 0$.

Lema A.29 *Um subgrupo aditivo em* $\mathbb{R}^n$ *é um reticulado se, e somente se, ele for discreto.* ■

Seja $\Lambda = \langle \mathbf{x}_1, \ldots, \mathbf{x}_n \rangle$ um reticulado em $\mathbb{R}^n$ gerado por n vetores linearmente independentes $\mathbf{x}_1, \ldots, \mathbf{x}_n$ sobre $\mathbb{R}$. Se

$$\mathbf{x}_i = (x_{i1}, \ldots, x_{in}),$$

então a matriz

$$M = [\mathbf{x}_i : 1 \leq i \leq n],$$

cujas linhas são os vetores $\mathbf{x}_i$ é chamada uma *matriz geradora* do reticulado Λ, e os elementos do reticulado Λ consistem de todos os vetores $\mathbf{u}M$, onde $\mathbf{u} \in \mathbb{Z}^n$.

O *determinante* do reticulado Λ é o valor absoluto do determinante da matriz geradora M, isto é,

$$d(\Lambda) = |\det(M)|.$$

O *volume fundamental* de um reticulado Λ é o volume de uma região fundamental, o qual será denotado por $V(\Lambda)$.

Lema A.30 *Seja Λ um reticulado de $\mathbb{R}^n$. Então $\mathbb{R}^n = \dot{\cup}_{\lambda\in\Lambda}(\lambda + T_{\mathbf{z}})$.* ■

Lema A.31 *Seja Λ um reticulado em $\mathbb{R}^n$. Então $V(\Lambda) = d(\Lambda) = V(T_{\mathbf{z}})$.* ■

Seja X um subconjunto de $\mathbb{R}^n$. Dizemos que X é *convexo* se o segmento

$$[\mathbf{x}, \mathbf{y}] = \{(1-t)\mathbf{x} + t\mathbf{y} :\forall\ \mathbf{x}, \mathbf{y} \in X \text{ e } t \in [0,1]\} \subset X.$$

Dizemos que X é *centrado simetricamente* se para todo $\mathbf{x} \in X$ tem-se $-\mathbf{x} \in X$.

Teorema A.32 (Minkowski) *Sejam Λ um reticulado de $\mathbb{R}^n$, X um subconjunto limitado, convexo e centrado simetricamente. Se*

$$V(X) > 2^n V(\Lambda),$$

então $X \cap \Lambda \neq \{\mathbf{0}\}$.

Prova. [2, Corolário, 17.8, p 149]. ■

Lema A.33 *A região $C = C(r)$ em*

$$\mathbb{R}^8 = \{(x_1, \ldots, x_8) : x_i \in \mathbb{R}\}$$

definida por

$$\sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2} + \sqrt{x_5^2 + x_6^2 + x_7^2 + x_8^2} \leq r$$

tem volume $\frac{\pi^4}{280} \cdot r^8$.

Prova. Seja

$$r_1 = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2} \text{ e } r_2 = \sqrt{x_5^2 + x_6^2 + x_7^2 + x_8^2}.$$

Então a região $C(r)$ é definida por

$$r_1 + r_2 \leq r.$$

Para cada ponto de r_1 à origem no $\mathbb{R}^4$ há uma região de volume $V(B_4(r - r_1))$ em $C(r)$. Assim, o volume de $C(r)$ é

$$\int_{B_4(r)} V(B_4(r - r_1)).$$

Vamos integrar em relação a r_1. Assim,

$$\begin{aligned} 2\pi^2 \int_{r_1=0}^{r} \frac{2\pi^2}{2}(r-r_1)^4 r_1^3 dr_1 &= \pi^4 \int_0^r (r-r_1)^4 r_1^3 dr_1 \\ &= \pi^4 \int_0^r (r-r_1)^2 (r-r_1)^2 r_1^3 dr_1 \\ &= \pi^4 \int_0^r (r^2 - 2rr_1 + r_1^2)(r^2 - 2rr_1 + r_1^2) r_1^3 dr_1 \\ &= \frac{\pi^4}{280} r^8. \end{aligned}$$

■

Lema A.34 *Seja X um subconjunto fechado de $\mathbb{R}^n$. Então X é convexo se, e somente se, $\frac{1}{2}(\mathbf{x}+\mathbf{y}) \in X$, para todos $\mathbf{x}, \mathbf{y} \in X$.*

Prova. Suponhamos que X é convexo. Então tomando $t = \frac{1}{2}$, obtemos

$$\left(1 - \frac{1}{2}\right)\mathbf{x} + \frac{1}{2}\mathbf{y} = \frac{1}{2}\mathbf{x} + \frac{1}{2}\mathbf{y} = \frac{1}{2}(\mathbf{x}+\mathbf{y}) \in X,$$

para todos $\mathbf{x}, \mathbf{y} \in X$. Reciprocamente, sejam $\mathbf{x}, \mathbf{y} \in X$ e

$$[\mathbf{x}, \mathbf{y}] = \{(1-t)\mathbf{x} + t\mathbf{y} : t \in [0,1]\}.$$

Queremos mostrar que $[x, y] \subset X$. Considere

$$\gamma : [0,1] \to X,$$

definida por $\gamma(t) = (1-t)\mathbf{x} + t\mathbf{y}$. É claro que γ é contínua. Seja

$$A = \{\frac{n}{2^m} : n, m \in \mathbb{N}\} \text{ e } B = A \cap [0,1].$$

Então, para qualquer $t \in B$, tem-se $\gamma(t) \in X$, pois $t \in B$ representa os pontos médio de $[x, y]$. Consideremos, agora, $\overline{B} = [0,1]$, isto é, B é denso em $[0,1]$. Assim, basta mostrar apenas que B é denso em $(0,1)$. Seja $I \subset (0,1)$ qualquer intervalo aberto. Então

$$B \cap I \neq \varnothing.$$

Seja $l(I) > 0$ o comprimento de I. Escolhendo um $n_0 \in \mathbb{N}$ e $a \in I$ tal que

$$\frac{1}{2^{n_0}} < \min\left\{a, \frac{l(I)}{4}\right\}.$$

Assim,

$$\lim_{m\to\infty} \frac{m}{2^{n_0}} = \frac{1}{2^{n_0}} \lim_{m\to\infty} m = \infty.$$

Seja

$$C = \{m \in \mathbb{N} : \frac{m}{2^{n_0}} < a, \text{ onde } I = (a, b)\}.$$

Então $1 \in C$ e existe um $k \in \mathbb{N}$ tal que $m \geq k$ com $m \notin C$. Portanto, C é um conjunto limitado. Logo, tomando $m_0 = \max C$, obtemos $\overline{\gamma(B)} = [x, y]$, onde

$$\gamma(B) = \{\gamma(t) : t \in B\} \text{ ou } \gamma(B) \subset X.$$

Seja $t \in [0, 1]$ qualquer. Então existe uma seqüência (t_n) em B tal que

$$\lim_{n\to\infty} t_n = t,$$

pois $\overline{B} = [0, 1]$. Portanto,

$$\lim_{n\to\infty} \gamma(t_n) = \gamma(t).$$

Como $\gamma(t_n) \in X$ e X é fechado temos que $\gamma(t) \in X$, isto é, X é convexo ■

Referências Bibliográficas

[1] Deutsch, J. I. "An alternate proof Cohn's four squares theorem," *J. Number Theory*, 104 (2004), pp 263 - 278.

[2] Endler, O. *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro, 1985.

[3] Garcia, A. L. e Lequain, Y., *Álgebra*: *Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[4] Gonçalves, A. *Introdução à Álgebra*. IMPA, Rio de Janeiro, 1979.

[5] G. H. Hardy and Wright, E. M., *An Introduction to the Theory of Numbers*. Oxford Science Publications,1979.

[6] Herstein, I. N., *Abstract Algebra*. Macmillan, 1990.

[7] MacLane, S. and Birkhoff, G. *Algebra*. Macmillan Company, 1968.

[8] Samuel, P., *Algebraic Theory of Numbers*. Hermann, Paris 1970.

[9] Silva, A. A., *Notas de Aulas*, Depto de Matemática, UFPB - Campus *I*.

[10] Stewart, I. N. and Tall, D. O., *Algebraic Number Theory*. Chapman and Hall, London, 1987.

[11] Weiss, E., *Algebraic Number Theory*, Dover, 1998.