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

Uma Prova de Geometria dos Números do Teorema dos Quatro-Quadrados de Götzky

por

Vilmar Vaz da Silva

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.

Outubro/2006

João Pessoa - PB

Uma Prova de Geometria dos Números do Teorema dos Quatro-Quadrados de Götzky

por

Vilmar Vaz da Silva

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. Antônio de Andrade e Silva - UFPB (Examinador)

Prof. Dr. Fernando Antônio Xavier de Sousa - UFPB (Examinador)

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

Outubro/2006

Agradecimentos

- A Deus, pois sem ele, nada seria.

- Ao Professor Dr. *Antônio de Andrade e Silva*, pois com sabedoria e respeito me auxiliou na elaboração deste trabalho.

- Ao Professor Dr. *Orlando Stanley Juriaans*, pela orientação, incentivo, compreensão e principalmente confiança.

- Ao Professor Dr. *Hélio Pires*, que em muitos momentos me ajudou de forma extremamente atenciosa.

- Ao Professor Dr. *Fernando Antônio Xavier de Sousa*, pelo incentivo e por idéias valorosas que engrandeceram este trabalho.

- .Aos funcionários da Pós-Graduação *Júnior e Graça*, pelo apoio logístico.

- Aos colegas do curso de mestrado, em especial aos amigos que sempre tiveram presentes nos momentos de maior dificuldade do curso:

- Anderson

- Carlos Henrique de Jesus

- Elisandra

- João de Sousa

- Ao meu pai *José Ricardo da Silva*, que sempre torceu pelo meu sucesso.

Dedicatória

À minha esposa Adriana Carla Soares Vaz e aos meus filhos Víctor Soares Vaz, Natália Soares Vaz e Letícia Soares Vaz, pois, são as pessoas que mais amo nessa vida .

Resumo

É conhecido que os inteiros algébricos totalmente positivos de alguns corpos numéricos são somas de quatro quadrados de inteiros algébricos desses corpos. O caso de $\mathbb{Q}(\sqrt{5})$ foi demonstrado por Götzky e os casos de $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$ foi demonstrado por Cohn. No presente trabalho apresentamos uma prova alternativa do teorema dos quatro quadrados de Götzky para $\mathbb{Q}(\sqrt{5})$, utilizando o método geométrico de Minkowski.

Abstract

It is known that the totally positive algebraic integers of some number fields they are sums of four squares of algebraic integers of those fields. The case of $\mathbb{Q}(\sqrt{5})$ was demonstrated by Götzky and the cases of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ was demonstrated by Cohn. In the present work we presented an alternative proof of the theorem of the four squares of Götzky for $\mathbb{Q}(\sqrt{5})$, using the geometric method of Minkowski.

Notação

R - Anel

$R[x]$ - Anel dos polinômios sobre R

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

I_L - Anel dos inteiros algébricos

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

$\mathbb{Z}_p[x]$ - Conjunto dos polinômios na variável x com coeficientes em $\mathbb{Z}_p$

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

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

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

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

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

$a \cdot R$ - Ideal gerado por a em R

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

$\text{mdc}(a, b)$ - Máximo dividor comum de a e b

$\int$ - Integral

χ - Função característica

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

$\mathbb{F}^\bullet$ - Grupo cíclico multiplicativo do corpo $\mathbb{F}$

$\mathbb{F}_p[x]$ - Anel dos polinômios sobre o corpo $\mathbb{F}_p$

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

$\partial(f)$ - Grau do polinômio f

$B_n(r)$ - bola do $\mathbb{R}^n$ de raio r e centro na origem

$[L : K]$ - Grau de L sobre K

f_α - Polinômio caracteristico de α

$p_{\alpha|K}$ - polinômio minimal de α sobre K

$\ker \phi$ - Núcleo da função ϕ

$\text{Im}\, \phi$ - Imagem da função ϕ

$\varphi\,|_A$ - Restrição da aplicação φ ao conjunto A

$|X|$ - Cardinalidade do conjunto X

$\mathfrak{N}(\mathfrak{a})$ - Norma do ideal $\mathfrak{a}$

$\|x\|$ - Norma de x

$|x|$ - Módulo de x

$n!$ - Fatorial do número natural n

$\equiv$ - Congruente

$|$ - Divide

$\simeq$ - Isomorfo

$\forall$ - Para todo

$\sum$ - Soma

$\prod$ - Produto

$\dot{\bigcup}$ - União disjunta

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

$\mathcal{T}_{L|K}(\alpha)$ - Traço de α em relação a $L \mid K$

$\mathcal{N}_{L|K}(\alpha)$ - Norma de α em relação a $L \mid K$

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

$disc_{L|K}(\alpha_1, \ldots, \alpha_n)$ - discriminante da n-upla $(\alpha_1, \ldots, \alpha_n)$

d_L - Discriminante do corpo L

$Vol(M)$ - Volume de M

Sumário

Introdução

O trabalho a seguir baseia-se no artigo intitulado Geometry of Numbers Proof of Götzky's Four-Squares Theorem, de Jesse Ira Deutsch, publicado em 2002 (ver [3]).

Vários foram os resultados de representação de dois quadrados e quatro quadrados para inteiros racionais estudados pelos matemáticos antigos; dentre eles está o famoso Teorema de Lagrange que afirma que todo inteiro positivo pode ser representado como a soma de quatro quadrados de inteiros. Este famoso resultado foi conjeturado pela primeira vez por Diofanto, um dos primeiros matemáticos gregos. Fermat, embora tenha tentado provar tal resultado, não obteve êxito, conseguindo apenas provar o teorema dos dois quadrados. Mais tarde, Euler aproveitando o resultado obtido por Fermat acrescentou resultados substânciais sobre o problema e, finalmente, em 1770, Lagrange deu a primeira demonstração completa do teorema, tendo como base o trabalho desenvolvido por Euler. No início do século XIX, Cauchy provou que todo inteiro racional positivo tem sido soma de três números triangulares, quatro quadrados, cinco números pentagonais, etc. Em 1928, Götzky provou que todo inteiro totalmente positivo em $\mathbb{Q}(\sqrt{5})$ é soma de quatro quadrados de inteiros algébricos daquele corpo. Em particular, Götzky mostrou que o número destas representações para um inteiro totalmente positivo $\alpha \in \mathbb{Q}(\sqrt{5})$ é

$$8 \cdot \sum_{(\nu)|\alpha} |N(\nu)| - 4 \cdot \sum_{2|(\nu)|\alpha} |N(\nu)| + 8 \cdot \sum_{4|(\nu)|\alpha} |N(\nu)| \ ,$$

onde N significa a norma do corpo e (ν) representa os ideais dividindo α. Aproximadamente em 1960, Cohn extendeu este trabalho para mostrar a existência de representações por somas de quadrados para $\mathbb{Q}(\sqrt{2})$ e $\mathbb{Q}(\sqrt{3})$. Além disso, ele mostrou que três quadrados são suficientes em um número de casos. Os teoremas de Götzky e Cohn tem sido demonstrados por meio da teoria de funções modulares para duas variáveis complexas e relacionados a funções theta. Embora os resultados de Götzky e Cohn exigiram conhecimentos das regiões fundamentais dos grupos modulares e cuidadosas estimativas dos

valores das funções theta, eles foram capazes de obter valores exatos para o número de tais representações.

No presente trabalho, uma demonstração alternativa mostrando a existência da representação de um inteiro racional como soma de quatro quadrados é feita utilizando o teorema do limite convexo de Minkowski da geometria dos números. Também o teorema clássico dos dois quadrados pode ser provado com técnicas muito semelhantes. Ainda neste trabalho, análogos destes teoremas são provados usando a técnica do limite convexo de Minkowski para representação por somas de quadrados no caso do corpo quadrático $\mathbb{Q}(\sqrt{5})$.

Daqui por diante, o desenvolvimento do nosso trabalho seguirá o seguinte roteiro:

- no capítulo 1 apresentamos a prova do teorema de Lagrange para representação de um racional inteiro como soma de quatro quadrados de inteiros, utilizando o Anel dos Quatérnios Inteiros de Hurwitz e suas propriedades;

- no capítulo 2 apresentamos o método geométrico, utilizando a geometria dos números, dando ênfase ao teorema de Minkowski para pontos de um reticulado e provamos o teorema de Lagrange através do referido método;

- finalmente, no capítulo 3 apresentamos o trabalho de Gesse Ira Deutch, onde nós utilizamos o método geométrico anteriormente citado e provamos o teorema de Götzki que afirma ser todo inteiro totalmente positivo do anel dos inteiros algébricos $I_{\mathbb{Q}(\sqrt{5})}$, uma soma de quatro quadrados de inteiros deste anel.

Capítulo 1

Teorema dos quatro quadrados para os inteiros racionais

Neste capítulo provaremos o famoso teorema de Lagrange o qual afirma que todo racional inteiro não negativo é soma de quatro quadrados de racionais inteiros.

1.1 Anel dos quatérnios reais

Nesta seção, apresentaremos um pouco da estrututura e das propriedades do anel dos quatérnios reais, que serão relevantes no decorrer deste capítulo.

Seja

$$Q = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3); \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}\}$$

Defina, para todos $x = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, $y = (\beta_0, \beta_1, \beta_2, \beta_3)$ em Q, as seguintes operações:

1. $x + y = (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \alpha_2 + \beta_2, \alpha_3 + \beta_3)$

2. $x \cdot y = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3, \alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2, \alpha_0\beta_2 + \alpha_2\beta_0 +$

$$+\alpha_3\beta_1 - \alpha_1\beta_3, \alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)$$

1. $(Q, +, \cdot)$ é um anel, denominado o *anel dos quatérnios reais*.

Observe ainda que fazendo as seguintes identificações:
$1 := (1, 0, 0, 0)$, $i := (0, 1, 0, 0)$, $j := (0, 0, 1, 0)$, $k := (0, 0, 0, 1)$, temos:

$$\begin{aligned} Q &= \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k; \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}, i^2 = j^2 = k^2 = ijk = -1, \\ ij &= -ji = k, jk = -kj = i, ki = -ik = j\} \end{aligned}$$

O leitor pode observar que Q é um anel não comutativo em que $0 = 0 + 0i + 0j + 0k$ e $1 = 1 + 0i + 0j + 0k$ funcionam, respectivamente, como o zero e o elemento unidade. Agora, se $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \neq 0$, então $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ não são todos nulos; como são reais, temos que $\beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$. Portanto:

$$y = \frac{\alpha_0}{\beta} - \frac{\alpha_1}{\beta} i - \frac{\alpha_2}{\beta} j - \frac{\alpha_3}{\beta} k \in Q$$

É fácil mostrar que $x \cdot y = 1$. Assim, os elementos não nulos de Q formam um grupo não abeliano com relação à multiplicação, sendo por isso denominado *anel com divisão* ou *anticorpo.*

Definição 1.1 *Para $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ em Q, o* conjugado *de x, indicado por x^*, é definido por*

$$x^* = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$$

Lema 1.2 *A conjugação em Q satisfaz:*

(1) $(x^*)^* = x$

(2) $(\delta x + \gamma y)^* = \delta x^* + \gamma y^*$, $\delta, \gamma \in \mathbb{R}$

(3) $(xy)^* = y^* x^*$

Prova.(1) e (2) segue diretamente da definição 1.1.

Em virtude de (2), para provar (3) basta fazê-lo para uma base de Q sobre os reais, a saber a base $1, i, j, k$. Observe:

$$\begin{aligned} i \cdot j = k &\implies (i \cdot j)^* = k^* = -k = j \cdot i = (-j) \cdot (-i) = j^* \cdot i^* \\ i \cdot k = -j &\implies (i \cdot k)^* = (-j)^* = j = k \cdot i = (-k) \cdot (-i) = k^* \cdot i^* \\ i^2 = -1 &\implies (i^2)^* = (-1)^* = -1 = (-i) \cdot (-i) = i^* \cdot i^* = (i^*)^2, \end{aligned}$$

analogamente para j e k. Portanto (3) é verdadeira para todas as combinações lineares dos elementos da base com coeficientes reais; então vale para x e y arbitrários em Q. ■

Definição 1.3 *Se $x \in Q$, então a* norma *de x, indicada por $N(x)$, é definida por*

$$N(x) = x \cdot x^*.$$

Notemos que se $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, então:

$$\begin{aligned} N(x) &= (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k) \\ &= \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2. \end{aligned}$$

Observação 1.4 *$N(0) = 0$ e $N(x) > 0$ se $x \neq 0$ em Q. Em particular, para todo número real α, $N(\alpha) = \alpha^2$. Se $x \neq 0$, observamos ainda que*

$$x^{-1} = \frac{1}{N(x)} \cdot x^*.$$

Lema 1.5 *Para todos $x, y \in Q$,*

$$N(x \cdot y) = N(x) \cdot N(y)$$

Demonstração.Pela própria definição de norma(1.3), temos:

$$N(x \cdot y) = (x \cdot y) \cdot (x \cdot y)^* = x \cdot y \cdot y^* \cdot x^*.$$

Contudo, $y \cdot y^* = N(y)$ é um número real e, portanto, está no centro de Q; em particular, ele comuta com x^*. Daí,

$$\begin{aligned} N(x \cdot y) &= (x \cdot y) \cdot (x \cdot y)^* = x \cdot y \cdot y^* \cdot x^* \\ &= (x \cdot x^*) \cdot (y \cdot y^*) = N(x) \cdot N(y). \end{aligned}$$

Portanto, $N(x \cdot y) = N(x) \cdot N(y)$ ■

Lema 1.6 (Identidade de Lagrange) *Se $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ e $\beta_0, \beta_1, \beta_2, \beta_3$ são números reais, então:*

$$\begin{aligned} (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2) \cdot (\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2) &= (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3)^2 + \\ &+ (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)^2 + \\ &+ (\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)^2 + \\ &+ (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)^2 \end{aligned}$$

Demonstração. Sejam

$$x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \text{ e } y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$$

Então, temos que

$$\begin{aligned} x \cdot y &= (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i + \\ &\quad +(\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)k. \end{aligned}$$

Pela definição 1.3 e o lema 1.5, temos

$$\begin{aligned} N(x \cdot y) &= N(x) \cdot N(y) = (\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2) \cdot (\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2) \\ &= (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3)^2 + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)^2 + \\ &\quad +(\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)^2 + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)^2. \end{aligned}$$

■

1.2 O anel dos quatérnios inteiros de Hurwitz

Nesta seção introduziremos o anel dos quatérnios inteiros de Hurwitz, que possui uma estrutura na qual o algorítmo da divisão à esquerda é válido, o que nos permitirá caracterizar seus ideais à esquerda.

Seja $\zeta = \frac{1}{2}(1 + i + j + k)$ e considere o conjunto

$$H = \{m_0\zeta + m_1 i + m_2 j + m_3 k \ ; \ m_0, m_1, m_2, m_3 \in \mathbb{Z}\}.$$

Lema 1.7 *H é um subanel de Q. Se $x \in H$, então $x^* \in H$ e $N(x)$ é um inteiro positivo para todo x não nulo em H.* ■

Definição 1.8 *H é chamado de* anel dos quatérnios inteiros de Hurwitz.

Os dois lemas seguintes são resultados simples obtidos da estrutura dos inteiros, porém importantes na demonstração do algorítmo da divisão que veremos a seguir.

Lema 1.9 *Sejam $t, n \in \mathbb{Z}$ com $n > 0$. Existem $x, r \in \mathbb{Z}$ tais que $t = x \cdot n + r$, onde*

$$-\frac{n}{2} \leq r \leq \frac{n}{2};$$

para este x,

$$|t - nx| = |r| \leq \frac{n}{2}.$$

Demonstração.Como $\mathbb{Z}$ é euclideano, existem $q, s \in \mathbb{Z}$ tais que

$$t = q \cdot n + s, \text{ com } s = 0 \text{ ou } |s| < n.$$

Se

$$0 \leq |s| \leq \frac{n}{2},$$

então $x = q$ e $r = s$ e finalizamos. Por outro lado, se

$$|s| \geq \frac{n}{2},$$

temos

$$t = (q+1) \cdot n + s - n \text{ se } s > 0 \text{ ou } t = (q-1) \cdot n + s + n \text{ se } s < 0.$$

Portanto, $x = q + 1$ e $r = s - n$ se $s > 0$ ou $x = q - 1$ e $r = s + n$ se $s < 0$. ■

Lema 1.10 *Sejam $t_0, t_1, t_2, n \in \mathbb{Z}$ com $n > 0$.Então, existe $k \in \mathbb{Z}$ tal que*

$$|t_0 + 2 \cdot t_1 - n \cdot (t_2 + 2 \cdot k)| \leq n.$$

Demonstração. Novamente do fato de $\mathbb{Z}$ ser euclideano, existem $p, s \in \mathbb{Z}$ tais que

$$t_0 + 2 \cdot t_1 = p \cdot n + s, \text{ com } 0 \leq s < n$$

Consideramos dois casos

1. se $p - t_2$ é par, então colocamos

   $$2 \cdot k = p - t_2$$

   e obtemos

   $$p = 2 \cdot k + t_2.$$

   Portanto,

   $$t_0 + 2 \cdot t_1 = (2 \cdot k + t_2) \cdot n + s$$

   e finalmente

   $$|t_0 + 2 \cdot t_1 - n \cdot (t_2 + 2 \cdot k)| = |s| = s < n.$$

2. se por outro lado, $p - t_2$ é ímpar, colocamos

$$2 \cdot k = p - t_2 + 1$$

ou seja

$$p = 2 \cdot k + t_2 - 1.$$

Daí, segue que

$$t_0 + 2 \cdot t_1 = (2 \cdot k + t_2 - 1) \cdot n + s = (2 \cdot k + t_2) \cdot n + s - n$$

o que nos leva a

$$|t_0 + 2 \cdot t_1 - n \cdot (t_2 + 2 \cdot k)| = |s - n| \leq n.$$

Logo, em ambos os casos, o lema segue. ■

Lema 1.11 (Algorítmo da divisão à esquerda-fraco) *Seja $a \in H$ e $n \in \mathbb{Z}_+^*$. Então existem dois elementos $c, d \in H$ tais que*

$$a = c \cdot n + d \ \ com \ \ N(d) < N(n).$$

Demonstração. Suponhamos que

$$a = t_0\zeta + t_1 i + t_2 j + t_3 k \ \text{ e } \ c = x_0\zeta + x_1 i + x_2 j + x_3 k,$$

onde x_0, x_1, x_2, x_3 são inteiros a serem determinados de maneira que

$$N(a - c \cdot n) < n^2 = N(n).$$

Mas observe que

$$\begin{aligned} a - c \cdot n &= \left(t_0\left(\frac{1+i+j+k}{2}\right) + t_1 i + t_2 j + t_3 k\right) - nx_0\left(\frac{1+i+j+k}{2}\right) - \\ &\quad -nx_1 i - nx_2 j - nx_3 k \end{aligned}$$

ou seja

$$\begin{aligned} a - c \cdot n &= \frac{1}{2}(t_0 - nx_0) + \frac{1}{2}(t_0 + 2t_1 - n(x_0 + 2x_1))i + \\ &\quad + \frac{1}{2}(t_0 + 2t_2 - n(x_0 + 2x_2))j + \frac{1}{2}(t_0 + 2t_3 - n(x_0 + 2x_3))k \end{aligned}$$

portanto

$$\begin{aligned} N(a - c \cdot n) &= \frac{(t_0 - nx_0)^2}{4} + \frac{(t_0 + 2t_1 - n(x_0 + 2x_1))^2}{4} + \\ &\quad + \frac{(t_0 + 2t_2 - n(x_0 + 2x_2))^2}{4} + \frac{(t_0 + 2t_3 - n(x_0 + 2x_3))^2}{4}. \end{aligned}$$

Pelos lemas 1.9 e 1.10 podemos tomar x_0, x_1, x_2 e x_3 tais que

$$|t_0 - nx_0| \leq \frac{n}{2} \text{ e } |t_0 + 2t_i - n(x_0 + 2x_i)| \leq n \text{ para } i = 1, 2, 3.$$

Segue então que

$$N(a - c \cdot n) \leq \frac{1}{16}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 = \frac{13}{16}n^2 < n^2 = N(n).$$

Logo, $a = c \cdot n + (a - c \cdot n)$ com $N(a - c \cdot n) < N(n)$. ■

Lema 1.12 (Algorítmo da divisão à esquerda-forte) *Sejam a e b em H com $b \neq 0$. Então existem dois elementos c e d em H tais que*

$$a = c \cdot b + d \text{ e } N(d) < N(b).$$

Demonstração. Pelo lema 1.7, $n = b \cdot b^*$ é um inteiro positivo e pelo lema 1.11, existe um $c \in H$ tal que

$$a \cdot b^* = c \cdot n + d_1, \text{ onde } d_1 \in H \text{ e } N(d_1) < N(n).$$

Assim,

$$N(a \cdot b^* - c \cdot n) = N(d_1) < N(n) \implies N(a \cdot b^* - c \cdot b \cdot b^*) < N(b \cdot b^*)$$

ou seja

$$N((a - c \cdot b) \cdot b^*) < N(b \cdot b^*) \implies N(a - c \cdot b) \cdot N(b^*) < N(b) \cdot N(b^*)$$

e então

$$N(a - c \cdot b) < N(b).$$

Colocando $d = a - c \cdot b \implies a = c \cdot b + d$ com $N(d) < N(b)$. ■

Lema 1.13 *Seja L um ideal à esquerda de H. Então existe um elemento $u \in L$ tal que todo elemento em L é um múltiplo à esquerda de u; em outras palavras, existe um $u \in L$ tal que todo $x \in L$ é da forma*

$$x = r \cdot u, \text{ onde } r \in H.$$

Demonstração. Se $L = (0)$, basta tomarmos $u = 0$.

Portanto, podemos assumir que $L \neq (0)$. Em virtude do lema 1.7 as normas dos elementos não nulos são inteiros positivos; logo, pelo princípio da boa ordenação para os naturais existe um elemento $u \neq 0$ em L cuja norma é mínima sobre os elementos não nulos de L. Se $x \in L$, pelo lema 1.12 existem $c, d \in H$ tais que

$$x = c \cdot u + d, \text{ onde } N(d) < N(u).$$

Como L é um ideal à esquerda de H, temos

$$c \cdot u \in L \text{ e } d = \underbrace{x}_{\in L} - \underbrace{c \cdot u}_{\in L} \in L.$$

Pela minimalidade de $N(u)$, segue que

$$N(d) = 0 \implies d = 0.$$

Logo, $x = c \cdot u$ com $c \in H$. ■

Lema 1.14 *Se $a \in H$, então*

$$a^{-1} \in H \iff N(a) = 1.$$

Demonstração. Se a e a^{-1} estão em H, então pelo lema 1.7 tanto $N(a)$ como $N(a^{-1})$ são inteiros positivos. No entanto, $a \cdot a^{-1} = 1$; portanto, pelo lema 1.5, temos

$$N(a) \cdot N(a^{-1}) = N(a \cdot a^{-1}) = N(1) = 1.$$

Logo, $N(a) = 1$.

Reciprocamente se $a \in H$ e $N(a) = 1$, então

$$a \cdot a^* = N(a) = 1 \implies a^{-1} \cdot a \cdot a^* = a^{-1} \implies a^* = a^{-1}.$$

Pelo lema 1.7 segue que $a^{-1} \in H$ ■

1.3 Teorema dos quatro quadrados

Nesta seção provaremos o principal resultado deste capítulo, ou seja, o teorema de Lagrange que inicialmente comentamos. Ainda apresentaremos alguns lemas no caminho deste.

Lema 1.15 *Seja R um anel com elemento unidade, R não necessariamente comutativo, tal que os únicos ideais à esquerda de R sejam (0) e R, então R é um anel com divisão.*

Demonstração. Devemos mostrar que se $0 \neq a \in R$, então existe b não nulo em R tal que $a \cdot b = 1$. Mas se $a \in R$ é não nulo, seja

$$I = \langle a \rangle = \{x \cdot a \ \ ; \ \ x \in R\}$$

o ideal à esquerda de R gerado por a. Como $I \neq (0)$, pois $a \in I$, temos que $I = R$. Como $1 \in R = I$, existe $b \in R$ tal que $b \cdot a = 1$.

Portanto, R é um anel com divisão. ■

Nosso próximo resultado será o clássico teorema de Wedderburn, que aqui não será demonstrado uma vez que necessitaria de muitos outros resultados da teoria dos corpos finitos; porém sua demonstração pode ser encontrada em [9].

Teorema 1.16 (Wedderburn) *Um anel finito com divisão é, necessariamente, um corpo.* ■

Consideremos agora os quatérnios W_p sobre $\mathbb{Z}_p$, onde p é um primo ímpar, ou seja:

$$W_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \ \ ; \ \ \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_p\}.$$

Observação 1.17 *W_p é um anel finito; além disso, como $p \neq 2$, W_p é não comutativo, por exemplo, $i \cdot j = -j \cdot i \neq j \cdot i$, uma vez que $-1 = p - 1 \neq 1$ em $\mathbb{Z}_p$.*

Consideremos ainda o ideal bilateral V em H definido por:

$$V = \{x_0\zeta + x_1 i + x_2 j + x_3 k \ \ ; \ \ p \,|\, x_0, x_1, x_2, x_3\}.$$

Lema 1.18 $\frac{H}{V} \simeq W_p$.

Demonstração. De fato, considere a aplicação

$$\varphi : \begin{cases} H & \longrightarrow & W_p \\ m_0\zeta + m_1 i + m_2 j + m_3 k & \longmapsto & \overline{m_0}\zeta + \overline{m_1} i + \overline{m_2} j + \overline{m_3} k \end{cases}$$

φ é claramente um homomorfismo sobrejetor e

$$\ker(\varphi) = \{v \in H \ ; \ \varphi(v) = 0\} = \{m_0\zeta + m_1 i + m_2 j + m_3 k \ ; \ p \,|\, m_0, m_1, m_2, m_3\} = V$$

Pelo teorema do homomorfismo, temos que:

$$\frac{H}{\ker(\varphi)} \simeq \mathrm{Im}(\varphi)$$

ou seja, $\frac{H}{V} \simeq W_p$. ■

Lema 1.19 (Artifício de Euler) *Se* $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$, *onde* x_0, x_1, x_2, x_3 *são inteiros, então* $a = y_0^2 + y_1^2 + y_2^2 + y_3^2$ *para certos inteiros* y_0, y_1, y_2, y_3.

Demonstração.Como $2a$ é par, então os x_i são todos pares, todos ímpares ou dois são pares e dois são ímpares. De qualquer forma, em todos os três casos podemos reordenar os x_i e agrupá-los de maneira tal que

$$y_0 = \frac{x_0 + x_1}{2} \ , \ y_1 = \frac{x_0 - x_1}{2} \ , \ y_2 = \frac{x_2 + x_3}{2} \ \text{ e } \ y_3 = \frac{x_2 - x_3}{2}$$

sejam todos inteiros. Mas

$$\begin{aligned} y_0^2 + y_1^2 + y_2^2 + y_3^2 &= \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2 \\ &= \frac{x_0^2 + 2x_0x_1 + x_1^2 + x_0^2 - 2x_0x_1 + x_1^2 + x_2^2 + 2x_2x_3 + x_3^2 + x_2^2 -}{4} \\ &\quad \frac{-2x_2x_3 + x_3^2}{4} \\ &= \frac{2x_0^2 + 2x_1^2 + 2x_2^2 + 2x_3^2}{4} = \frac{1}{2}\left(x_0^2 + x_1^2 + x_2^2 + x_3^2\right) \\ &= \frac{1}{2} \cdot 2a = a. \end{aligned}$$

Portanto, o lema segue. ■

Agora estamos prontos para provarmos o nosso principal resultado.

Teorema 1.20 (Lagrange) *Todo inteiro positivo pode ser expresso como uma soma de quadrados de quatro inteiros.*

Demonstração. Como todo inteiro decompõe-se num produto de números primos, em vista do lema 1.6, o teorema resume-se a provar que todo primo é soma de quatro quadrados. Observe que

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

Assim, sem perda de generalidade podemos admitir que o número primo seja ímpar.

Seja p um número primo ímpar e consideremos os quatérnios W_p sobre $\mathbb{Z}_p$, ou seja

$$W_p = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \ \ ; \ \ \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}_p\}.$$

Pela observação 1.17 W_p é finito e não comutativo e pelo teorema 1.16, ele não pode ser um anel com divisão, pois, caso contrário seria um corpo.

Pelo lema 1.15 W_p possui um ideal à esquerda que não é (0) e nem W_p.

Agora pelo lema 1.18 temos que $\frac{H}{V} \simeq W_p$, onde

$$V = \{x_0\zeta + x_1 i + x_2 j + x_3 k \ \ ; \ \ p \mid x_0, x_1, x_2, x_3\}.$$

Daí, temos que V não pode ser um ideal maximal à esquerda em H, pois, caso contrário, $\frac{H}{V} \simeq W_p$ não teria nenhum ideal à esquerda além de (0) e W_p, ou seja W_p seria um anel com divisão, o que seria um absurdo.

Assim, existe um ideal à esquerda L de H satisfazendo:

$$L \neq H \ , \ L \neq V \ \text{ e } \ L \supset V.$$

Pelo lema 1.13 existe um elemento $u \in L$ tal que todo elemento em L seja um múltiplo à esquerda de u. Observe ainda que

$$p = 2p\zeta - pi - pj - pk \in V \subset L.$$

Ou seja, $p \in L$, donde $p = c \cdot u$ para algum $c \in H$. Como $u \notin V$, c não pode possuir um inverso em H, caso contrário, $u = c^{-1} \cdot p$ estaria em V. Assim, pelo lema 1.14, $N(c) > 1$. Como $L \neq H$, u não pode ter um inverso em H. De fato, pois se assim não fosse, teríamos:

$$u^{-1} \cdot u = 1 \in L \implies L = H.$$

Portanto, novamente pelo lema 1.14 $N(u) > 1$. Como $p = c \cdot u$, temos pelo lema 1.5,

$$N(p) = p^2 = N(c \cdot u) = N(c) \cdot N(u).$$

Como c e u são dois elementos não nulos de H, então pelo lema 1.7 $N(c)$ e $N(u)$ são inteiros positivos e sendo $N(c), N(u) > 1$ e divisores de p^2, então

$$N(c) = N(u) = p.$$

Como $u \in H$,

$$u = m_0\zeta + m_1 i + m_2 j + m_3 k \ , \ \text{ onde } \ m_0, m_1, m_2, m_3 \in \mathbb{Z};$$

assim:

$$\begin{aligned} 2u &= 2m_0\zeta + 2m_1 i + 2m_2 j + 2m_3 k \\ &= m_0 + m_0 i + m_0 j + m_0 k + 2m_1 i + 2m_2 j + 2m_3 k \\ &= m_0 + (2m_1 + m_0)i + (2m_2 + m_0)j + (2m_3 + m_0)k \end{aligned}$$

e segue que

$$N(2u) = N(2)N(u) = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2$$

ou seja,

$$4p = m_0^2 + (2m_1 + m_0)^2 + (2m_2 + m_0)^2 + (2m_3 + m_0)^2.$$

Como $4p$ é soma de quatro quadrados, então pelo lema 1.19 $2p$ e portanto p também o é. Logo,

$$p = a_0^2 + a_1^2 + a_2^2 + a_3^2 \ ,$$

para alguns inteiros a_0, a_1, a_2 e a_3. ■

Capítulo 2

Método Geométrico para a prova do Teorema Clássico de Soma de Quatro Quadrados

Neste capítulo apresentaremos uma prova alternativa do Teorema clássico dos quatro quadrados utilizando um método geométrico bastante simples, porém muito interessante.

2.1 Reticulados

Nesta seção apresentaremos noções básicas da geometria dos números, em particular, estudaremos os reticulados que são subgrupos aditivos e discretos do $\mathbb{R}^n$, em vista de demonstrarmos o famoso teorema de Minkowski para pontos de um reticulado.

Seja L um $\mathbb{R}$ - espaço de dimensão n, isto é, isomorfo ao $\mathbb{R}$ - espaço $\mathbb{R}^n$. Distinguimos em L uma base $e_1, e_2, \ldots, e_n$(por exemplo, $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$ no caso em que $L = \mathbb{R}^n$).

Definição 2.1 *Sejam* $x = \xi_1 \cdot e_1 + \cdots + \xi_n \cdot e_n$ *e* $y = \eta_1 \cdot e_1 + \cdots + \eta_n \cdot e_n$ *elementos de* L. *Definimos:*

1. *o* produto escalar *entre* x *e* y, *denotado como* (x, y), *por*

$$(x, y) = \xi_1 \cdot \eta_1 + \cdots + \xi_n \cdot \eta_n.$$

2. *o comprimento de* x, *representado por* $\|x\|$, *como sendo*

$$\|x\| = \sqrt{(x, x)} = \sqrt{\xi_1^2 + \cdots + \xi_n^2}$$

3. *a bola de centro* 0 *e raio* ρ*, indicada como* B_ρ*, por*

$$B_\rho = \{x \in L \ ; \ \|x\| \leq \rho\}.$$

Observação 2.2 *As definições acima são naturais em vista do isomorfismo acima mencionado.*

Dados $z_1, \ldots, z_m \in L$ com $m \leq n$, consideramos os conjuntos:

$$M = \mathbb{Z} \cdot z_1 + \cdots + \mathbb{Z} \cdot z_m = \left\{ \sum_{i=1}^{m} a_i \cdot z_i \ ; \ a_1, \ldots, a_m \in \mathbb{Z} \right\}$$

e

$$T_z = \left\{ \sum_{i=1}^{m} \rho_i \cdot z_i \ ; \ 0 \leq \rho_i < 1 (i = 1, \ldots, m) \right\}$$

Definição 2.3 *Diremos que* M *é um* reticulado *de* L *quando* $z_1, \ldots, z_m$ *forem linearmente independentes sobre* $\mathbb{R}$*; neste caso, chamamos* $\{z_1, \ldots, z_m\}$ *uma base associada ao reticulado* M*.*

Definição 2.4 *Quando* M *é um reticulado com base* $\{z_1, \ldots, z_m\}$*, o conjunto* T_z *é chamado de* malha fundamental *associada a esta base.*

Exemplo 2.5 *Seja* $L = \mathbb{R}^2$ *e* $M = \mathbb{Z} \cdot v_1 + \mathbb{Z} \cdot v_2$*, onde* $v_1 = (1, 1)$ *e* $v_2 = (2, 1)$*. Observe que estes vetores são claramente linearmente independentes sobre* $\mathbb{R}$ *e pela definição 2.3 acima,* M *é um reticulado.Observe ainda que*

$$M = \left\{ (x + 2y, x + y) \in \mathbb{R}^2 \ , \quad onde \ x, y \in \mathbb{Z} \right\}$$

Definição 2.6 *Diremos que um subconjunto* C *de* L *é* limitado*, se* $C \subseteq B_\rho$ *para algum* $\rho > 0$*.*

Definição 2.7 *Um subconjunto* D *de* L *é* discreto*, se* $D \cap B_\rho$ *for finito para todo* $\rho > 0$*; neste caso,* $D \cap C$ *é finito, qualquer que seja o subconjunto limitado* C *de* L*.*

O resultado seguinte nos permite concluir quando um dado subconjunto M de L é um reticulado, sem a necessidade de conhecermos uma base deste.

Proposição 2.8 *Um subconjunto* M *de* L *será um reticulado de* L *se, e somente se, for um grupo em relação à adição e for discreto.*

Demonstração. Suponhamos que M seja um reticulado de L.

Então, claramente, M é um grupo aditivo. Suponhamos que $v_1, \ldots, v_m$ formem uma base do reticulado M; então

$$m \leq n,$$

e existem $v_{m+1}, \ldots, v_n \in L$ tais que $v_1, \ldots, v_n$ são linearmente independentes sobre $\mathbb{R}$ e, portanto, formam uma base de um reticulado M' que contém M. Para mostrar que M é discreto, basta provar que M' o é. Se $w_1, \ldots, w_n$ formarem a base dual de $v_1, \ldots, v_n$, isto é,

$$(v_i, w_j) = \delta_{ij} (i, j = 1, \ldots, n);$$

então para todo $z = a_1 v_1 + \cdots + a_n v_n \in M'$ teremos que

$$\begin{aligned} (z, w_j) &= (a_1 v_1 + \cdots + a_j v_j + \cdots + a_n v_n, w_j) \\ &= \underbrace{a_1(v_1, w_j) + \cdots + a_{j-1}(v_{j-1}, w_j)}_{=0} + a_j \underbrace{(v_j, w_j)}_{=1} + \\ &\quad + \underbrace{a_{j+1}(v_{j+1}, w_j) + \cdots + a_n(v_n, w_j)}_{=0} \end{aligned}$$

Daí,

$$(z, w_j) = a_j (j = 1, \ldots, n).$$

Para todo $\rho > 0$ e todo $z \in M' \cap B_\rho$ temos que

$$\underbrace{|a_j|}_{\in \mathbb{Z}} = |(z, w_j)| \leq \|z\| \cdot \|w_j\| \leq \rho \cdot \|w_j\| \, (j = 1, \ldots, n);$$

logo, $M' \cap B_\rho$ é finito e portanto, M' é discreto.

Por outro lado, seja M um grupo aditivo e discreto. Suponhamos que $u_1, \ldots, u_m$ formem um sistema maximal de elementos de M linearmente independentes sobre $\mathbb{R}$; então $u_1, \ldots, u_m$ formam uma base do reticulado $M_0 = \mathbb{Z} \cdot u_1 + \cdots + \mathbb{Z} \cdot u_m$. Sendo T_u a malha fundamental associada a esta base, temos que

$$(M \cap T_u) + M_0 \subseteq M,$$

e como todo $x \in M$ é linearmente dependente(sobre $\mathbb{R}$) de $u_1, \ldots, u_m$, temos

$$(M \cap T_u) + M_0 = M \ ;$$

logo,

$$x = \sum_{i=1}^{m} a_i \cdot u_i + \sum_{i=1}^{m} \rho_i \cdot u_i \ \text{ com } \ a_i \in \mathbb{Z} \ \text{ e } \ 0 \leq \rho_i < 1 (i = 1, \ldots, m),$$

e assim

$$\sum_{i=1}^{m} \rho_i \cdot u_i = \left(x - \sum_{i=1}^{m} a_i \cdot u_i \right) \in M \cap T_u.$$

Considerando o homomorfismo canônico

$$\varphi : \begin{cases} M & \longrightarrow & \frac{M}{M_0} \\ m & \longmapsto & m + M_0 \end{cases},$$

concluímos que $\varphi \Big|_{M \cap T_u}$ é sobrejetivo. Como M é discreto e T_u é limitado, temos que $M \cap T_u$ é finito; logo $\frac{M}{M_0}$ também o é. Denotando por g a ordem de $\frac{M}{M_0}$, temos:

$$M \subseteq g^{-1} \cdot M_0 = \mathbb{Z} \cdot u_1' + \cdots + \mathbb{Z} \cdot u_m', \text{ onde } u_i' = g^{-1} \cdot u_i (i = 1, \ldots, m).$$

Portanto, M é um $\mathbb{Z}$-módulo livre, de um posto $k \leq m$, logo possui uma base

$$\{v_1, \ldots, v_k\}.$$

Das inclusões

$$M_0 \subseteq M \subseteq g^{-1} \cdot M_0$$

resulta que os $\mathbb{R}$-espaços gerados por estes $\mathbb{Z}$-módulos coincidem, isto é,

$$\mathbb{R} \cdot u_1 + \cdots + \mathbb{R} \cdot u_m = \mathbb{R} \cdot v_1 + \cdots + \mathbb{R} \cdot v_k,$$

donde concluímos que $k = m$ e que $v_1, \ldots, v_k$ são linearmente independentes sobre $\mathbb{R}$. Portanto, M é um reticulado de L. ■

Dado um reticulado M consideramos, além da malha fundamental T_v, também as outras malhas $z + T_v (z \in M)$, associadas a uma base $\{v_1, \ldots, v_m\}$ do reticulado M. Mostraremos que todo conjunto limitado intersecta apenas um número finito destas malhas.

Lema 2.9 *Seja T_v a malha fundamental associada à base $\{v_1, \ldots, v_m\}$ do reticulado M, e seja C um subconjunto limitado de L. Então $C \cap (z + T_v) = \varnothing$ para quase todos os $z \in M$.*

Demonstração. Para todo

$$t = \sum_{i=1}^{m} \rho_i \cdot v_i \in T_v$$

temos, pela desigualdade triangular, que:

$$\|t\| \leq \sum_{i=1}^{m} \|\rho_i \cdot v_i\| = \sum_{i=1}^{m} |\rho_i| \cdot \|v_i\| \leq \tau, \text{ onde } \tau = \sum_{i=1}^{m} \|v_i\| .$$

Supondo, sem perda de generalidade, que $C = B_\rho$ para algum $\rho > 0$, consideramos $z \in M$ tal que

$$B_\rho \cap (z + T_v) \neq \varnothing \ ;$$

digamos $z + t = x \in B_\rho$ para algum $t \in T_v$; então:

$$\|z\| = \|x - t\| \leq \|x\| + \|t\| \leq \rho + \tau \ ;$$

logo $z \in B_{\rho+\tau}$. Como M é discreto, pela proposição 2.8, o conjunto $M \cap B_{\rho+\tau}$ é finito, donde resulta a afirmação. ■

Teorema 2.10 *Seja L um $\mathbb{R}$-espaço de dimensão n e M um reticulado em L com base $\{v_1, \ldots, v_m\}$. As seguintes condições são equivalentes:*

(i) $m = n$;

(ii) *Existe um subconjunto limitado C de L tal que* $L = \bigcup_{z \in M} (z + C)$.

Neste caso temos, em particular, que $L = \bigcup_{z \in M} (z + T)$*(reunião disjunta), sendo T a malha fundamental associada a uma base de M.*

Demonstração. (i) $\Longrightarrow$ (ii) Para todo $x \in L$, temos que:

$$x = \sum_{i=1}^{n} a_i \cdot v_i + \sum_{i=1}^{n} \rho_i \cdot v_i \text{ com } a_i \in \mathbb{Z} \text{ e } 0 \leq \rho_i < 1 (i = 1, \ldots, n);$$

logo,

$$L = \bigcup_{z \in M} (z + T_v).$$

A reunião é disjunta, pois de

$$\sum_{i=1}^{n} a_i \cdot v_i + \sum_{i=1}^{n} \rho_i \cdot v_i = \sum_{i=1}^{n} a'_i \cdot v_i + \sum_{i=1}^{n} \rho'_i \cdot v_i$$

resulta que

$$a_i + \rho_i = a'_i + \rho'_i (i = 1, \ldots, n)$$

e, portanto

$$a_i = a'_i \text{ e } \rho_i = \rho'_i \ , \text{ para } i = 1, \ldots, n.$$

(ii) $\Longrightarrow$ (i) Suponha que $m < n$. Então, a base $\{v_1, \ldots, v_m\}$ de M, com $m < n$, pode ser completada até uma base $\{v_1, \ldots, v_n\}$ do $\mathbb{R}$-espaço L. Se $w_1, \ldots, w_n$ formarem a base dual de $v_1, \ldots, v_n$, então $(z, w_n) = 0$ para todo $z \in M$.

Seja $\rho > 0$ tal que $C \subseteq B_\rho$, e seja $y = \rho' \cdot w_n$ para algum $\rho' > \rho$. De (ii) resulta que

$$y = z + c \ , \ \text{com} \ z \in M \ \text{e} \ c \in C.$$

Como $(z, y) = 0$, concluimos que

$$\|y\|^2 = (z + c, y) = (z, y) + (c, y) = (c, y) \leq \|c\| \cdot \|y\| \leq \rho \cdot \|y\| \, ;$$

então,

$$\|y\| \leq \rho,$$

em contradição com $\|y\| = \|\rho' \cdot w_n\| = \rho'$. ■

2.2 O Teorema de Minkowski

O principal objetivo desta seção é a prova do Teorema de Minkowski e, para tanto necessitamos de algumas propriedades do volume em L, transferidas para o mesmo pelo isomorfismo natural com o $\mathbb{R}^n$ por meio da base distinguida $e_1, \ldots, e_n$.

Lema 2.11 *Para subconjuntos C de L que são reuniões finitas de paralelepípedos, valem as seguintes propriedades:*

a) $Vol(T_v) = |\det(\alpha_{ij})|$, *sendo* $v_i = \sum_{j=1}^{n} \alpha_{ij} \cdot e_j (i = 1, \ldots, n \ ; \alpha_{ij} \in \mathbb{R})$;

b) $Vol(x + C) = Vol(C)$ *para qualquer* $x \in L$;

c) $Vol(\gamma \cdot C) = \gamma^n \cdot Vol(C)$ *para qualquer* $\gamma \in \mathbb{R}$, $\gamma > 0$;

d) *Se* $C \cap C' = \varnothing$ *então* $Vol(C \cup C') = Vol(C) + Vol(C')$. ■

Lema 2.12 $v_1, \ldots, v_n \in L$ *formarão uma base de um reticulado em L se, e somente se,* $Vol(T_v) \neq 0$.

Demonstração. Segue imediatamente do item a) do lema anterior. ■

Lema 2.13 *Seja* $w_i = \sum_{j=1}^{n} w_{ij} \cdot v_j (i = 1, \ldots, n)$, *com* $w_{ij} \in \mathbb{R}$. *Então:*

$$Vol(T_w) = |\det(w_{ij})| \cdot Vol(T_v)$$

Demonstração. De fato, observe que:

$$\begin{aligned}
w_1 &= w_{11}v_1 + \cdots + w_{1n}v_n \\
&= w_{11}(\alpha_{11}e_1 + \cdots + \alpha_{1n}e_n) + \cdots + w_{1n}(\alpha_{n1}e_1 + \cdots + \alpha_{nn}e_n) \\
&= (w_{11}\alpha_{11} + \cdots + w_{1n}\alpha_{n1})e_1 + \cdots + (w_{11}\alpha_{1n} + \cdots + w_{1n}\alpha_{nn})e_n \\
w_2 &= w_{21}v_1 + \cdots + w_{2n}v_n \\
&= w_{21}(\alpha_{11}e_1 + \cdots + \alpha_{1n}e_n) + \cdots + w_{2n}(\alpha_{n1}e_1 + \cdots + \alpha_{nn}e_n) \\
&= (w_{21}\alpha_{11} + \cdots + w_{2n}\alpha_{n1})e_1 + \cdots + (w_{21}\alpha_{1n} + \cdots + w_{2n}\alpha_{nn})e_n \\
&\vdots \\
w_n &= w_{n1}v_1 + \cdots + w_{nn}v_n \\
&= w_{n1}(\alpha_{11}e_1 + \cdots + \alpha_{1n}e_n) + \cdots + w_{nn}(\alpha_{n1}e_1 + \cdots + \alpha_{nn}e_n) \\
&= (w_{n1}\alpha_{11} + \cdots + w_{nn}\alpha_{n1})e_1 + \cdots + (w_{n1}\alpha_{1n} + \cdots + w_{nn}\alpha_{nn})e_n
\end{aligned}$$

Pela parte a) do lema (2.11), temos:

$$Vol(T_w) = |\det(c_{ij})|, \text{ onde } c_{ij} = \sum_{k=1}^{n} w_{ik}\alpha_{kj}$$

ou seja,

$$Vol(T_w) = |\det[(w_{ij}) \cdot (\alpha_{ij})]| = |\det(w_{ij})| \cdot |\det(\alpha_{ij})|.$$

Portanto, $Vol(T_w) = |\det(w_{ij})| \cdot Vol(T_v)$. ■

Observação 2.14 *Obviamente,* $w_1, \ldots, w_n$ *e* $v_1, \ldots, v_n$ *formarão bases do mesmo reticulado se, e somente se,* $w_{ij} \in \mathbb{Z}(i, j = 1, \ldots, n)$ *e* $\det(w_{ij}) \in \{-1, 1\}$.

Lema 2.15 *Para todas as bases* $v_1, \ldots, v_n$ *de um reticulado* M, *os volumes* $Vol(T_v)$ *coincidem.*

Demonstração. Segue imediatamente do lema 2.13 e da observação 2.14. ■

Definição 2.16 *Seja* M *um reticulado em* L. *O* volume *de* M, *representado por* $Vol(M)$, *é definido como sendo o volume da malha fundamental associada a uma base deste reticulado, ou seja:*

$$Vol(M) = Vol(T_v),$$

onde $v_1, \ldots, v_n$ *formam uma base de* M.

Observação 2.17 *Pela parte b) do lema 2.11 observamos que o* $Vol(M)$ *é igual ao* $Vol(z+T_v)$ *de todas as malhas associadas a* $v_1, \ldots, v_n (z \in M)$.

O nosso próximo resultado afirma que os conjuntos $z + C(z \in M)$, obtidos de C por deslocamento ao longo de um reticulado M, serão disjuntos, dois a dois, somente quando C for suficientemente pequeno. Observamos também que o mesmo será fundamental para a demonstração do Teorema de Minkowski que decorrerá como um corolário.

Teorema 2.18 *Seja* $C \subseteq L$ *tal que* $Vol(C)$ *seja definido e seja* M *um reticulado n-dimensional de* L. *Se os conjuntos* $z + C(z \in M)$ *forem disjuntos dois a dois, então* $Vol(C) \leq Vol(M)$.

Demonstração. Seja T a malha fundamental associada a uma base de M. Pelo teorema 2.10, temos que

$$L = \bigcup_{z \in M} (z + T),$$

logo,

$$C = C \cap L = C \cap \left(\bigcup_{z \in M} (z + T) \right) = \bigcup_{z \in M} (C \cap (z + T)),$$

sendo ambas as reuniões disjuntas. Pelo lema 2.9 existem $z_1, \ldots, z_r \in M$ tais que

$$C \cap (z + T) = \varnothing,$$

para todos os $z \in M \setminus \{z_1, \ldots, z_r\}$; logo:

$$C = \bigcup_{i=1}^{\bullet r} (C \cap (z_i + T)) .$$

Como, por hipótese, $-z_i + C (i = 1, \ldots, r)$ são disjuntos dois a dois, a reunião

$$\bigcup_{i=1}^{r} ((-z_i + C) \cap T)$$

também é disjunta. Finalmente:

$$C \cap (z_i + T) = ((-z_i + C) \cap T) + z_i \ (i = 1, \ldots, r).$$

De fato:

$$a \in C \cap (z_i + T) \implies a \in C \text{ e } a \in (z_i + T).$$

Mas,

$$a = \underbrace{a - z_i}_{\in(-z_i+C)\cap T} + z_i \implies a \in ((-z_i + C) \cap T) + z_i$$

Por outro lado,

$$a \in ((-z_i + C) \cap T) + z_i \implies a = b + z_i, \text{ com } b \in (-z_i + C) \cap T$$

daí, $a \in C \cap (z_i + T)$. Logo:

$$\begin{aligned} Vol(C) &= Vol\left(\dot{\bigcup_{i=1}^{r}}(C \cap (z_i + T))\right) \\ &= \sum_{i=1}^{r} Vol(C \cap (z_i + T)) = \sum_{i=1}^{r} Vol((-z_i + C) \cap T) \\ &= Vol\left(\bigcup_{i=1}^{r}(-z_i + C) \cap T\right) \leq Vol(T) = Vol(M). \end{aligned}$$

Portanto, $Vol(C) \leq Vol(M)$. ■

Definição 2.19 *Um subconjunto C de L será chamado* centralmente simétrico *se, para qualquer $c \in C$, tivermos que $-c \in C$.*

Definição 2.20 *Um subconjunto C de L será chamado* convexo *se para quaisquer $c, c' \in C$, o conjunto*

$$\{\rho \cdot c + (1 - \rho) \cdot c' \ ; \ 0 \leq \rho \leq 1\}$$

estiver contido em C.

Exemplo 2.21 *Seja $L = \mathbb{R}^2$. Considere o seguinte subconjunto C de L:*

$$C = \{(x, y) \in \mathbb{R}^2 \ ; \ x^2 + y^2 \leq r^2 \ \text{ onde } r \in \mathbb{R}_+^*.$$

Observe que C é a bola do $\mathbb{R}^2$ de centro na origem e raio r e é claramente convexo e centralmente simétrico.

Mais geralmente, temos:

Teorema 2.22 *Toda bola $B \subset \mathbb{R}^n$ de centro 0 e raio $r > 0$ é convexa e centralmente simétrica.*

Demonstração. Seja B a bola fechada do $\mathbb{R}^n$ de centro 0 e raio $r > 0$, ou seja:

$$B = B_n(r) = \{x \in \mathbb{R}^n \ ; \ \|x\| \leq r\}.$$

Observe que se $x \in B$, então:

$$\|-x\| = \|(-1) \cdot x\| = |-1| \cdot \|x\| = \|x\| \leq r \implies (-x) \in B.$$

Portanto, B é centralmente simétrica. Por outro lado, se $x, y \in B$ então

$$\|x\| \leq r \ \text{ e } \ \|y\| \leq r.$$

Para qualquer $t \in [0, 1]$, temos:

$$\|(1-t)x + ty\| \leq \|(1-t)x\| + \|ty\| = (1-t)\|x\| + t\|y\| \leq (1-t)r + tr = r.$$

Logo, B também é convexa. ■

Corolário 2.23 (Teorema de Minkowski) *Seja C um subconjunto convexo, centralmente simétrico de L tal que $Vol(C)$ seja definido, e seja M um reticulado n-dimensional em L. Se*

$$Vol(C) > 2^n \cdot Vol(M),$$

então

$$C \cap (M \setminus \{0\}) \neq \varnothing.$$

Demonstração. Pelo ítem c) do lema 2.11, temos:

$$Vol\left(\frac{1}{2} \cdot C\right) = 2^{-n} \cdot Vol(C) > Vol(M),$$

e pelo teorema 2.18, concluimos que os conjuntos

$$\frac{1}{2} \cdot C + z (z \in M)$$

não são disjuntos dois a dois, isto é, existem $z_1, z_2 \in M$, $z_1 \neq z_2$, e $c_1, c_2 \in C$ tais que

$$\frac{1}{2} \cdot c_1 + z_1 = \frac{1}{2} \cdot c_2 + z_2.$$

Como C é centralmente simétrico e convexo, temos que:

$$-c_1 \in C \ \text{ e } \ z_1 - z_2 = \frac{1}{2} \cdot c_2 + \left(1 - \frac{1}{2}\right) \cdot (-c_1) \in C \cap (M \setminus \{0\}).$$

Logo, $C \cap (M \setminus \{0\}) \neq \varnothing$. ■

2.3 Soma de Dois Quadrados

Nesta seção trataremos basicamente do problema de representação de um primo racional como soma de dois quadrados, utilizando para isto a geometria dos números. Apresentaremos, inicialmente, alguns conceitos e resultados da teoria dos grupos que se adequam ao contexto.

Definição 2.24 *Seja $p \in \mathbb{Z}$ um número primo ímpar; $a \neq 0$ é dito um* resto quadrático *de p se existe um inteiro x tal que $x^2 \equiv a \bmod p$. Caso contrário, a é dito um* não-resto quadrático.

Lema 2.25 *Os restos quadráticos* $\bmod p$ *formam um subgrupo multiplicativo do grupo multiplicativo $\mathbb{Z}_p^*$ de ordem $\frac{p-1}{2}$.* ■

Lema 2.26 *Seja $S = \{y^2 + 1 \ ; \ y \in \mathbb{Z}\}$; então existe $z \in S$ tal que z não é um quadrado módulo p.*

Demonstração. Suponha que S possua apenas quadrados módulo p. Seja $y \in \mathbb{Z}$ tal que y seja um quadrado módulo p, ou seja:

$$y \equiv x^2 (\bmod p) \text{ com } x \in \mathbb{Z} \implies y + 1 \equiv x^2 + 1 (\bmod p)$$

Como $(x^2 + 1) \in S$, então

$$x^2 + 1 \equiv t^2 (\bmod p) \implies y + 1 \equiv x^2 + 1 \equiv t^2 (\bmod p)$$

ou seja, $y + 1$ é um quadrado módulo p. Portanto, por indução, todo inteiro positivo é um quadrado módulo p, o que é um absurdo, pois, pelo lema anterior, apenas metade dos inteiros entre 1 e $p - 1$ o são.

Logo, existe $z \in S$ tal que z não é um quadrado módulo p. ■

Lema 2.27 *Se n_1 e n_2 são não-restos quadráticos, então $n_1 \cdot n_2$ é um resto quadrático.* ■

Lema 2.28 *Se p é um número primo tal que $p \equiv 1 \bmod(4)$, então -1 é um resto quadrático* $\bmod p$.

Demonstração. Seja

$$x = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot \frac{p-1}{2}.$$

Como $p-1=4n(n\in\mathbb{Z})$, neste produto x existe um número par de têrmos, e conseqüentemente

$$x=(-1)\cdot(-2)\cdot(-3)\cdot\cdots\cdot\left(-\left(\frac{p-1}{2}\right)\right).$$

Mas,

$$\begin{cases} p-1\equiv -1 \bmod p \\ p-2\equiv -2 \bmod p \\ \quad\vdots \\ p-\frac{p-1}{2}\equiv -\frac{p-1}{2} \bmod p \implies \frac{p+1}{2}\equiv -\frac{p-1}{2} \bmod p \end{cases}$$

de modo que

$$\begin{aligned} x^2 &\equiv \left(1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}\right)\cdot(-1)\cdot(-2)\cdot\cdots\cdot\left(-\left(\frac{p-1}{2}\right)\right) \bmod p \\ &\equiv 1\cdot 2\cdot\cdots\cdot\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot\cdots\cdot(p-1) \bmod p \\ &\equiv (p-1)! \bmod p. \end{aligned}$$

Pelo teorema de Wilson, temos que

$$(p-1)!\equiv -1 \bmod p$$

e, portanto $x^2\equiv -1 \bmod p$. ■

Teorema 2.29 *Todo primo racional p para o qual -1 é um resto quadrático tem uma representação $p=x^2+y^2$ onde $x,y\in\mathbb{Z}$.*

Demonstração. Como -1 é resto quadrático $\bmod p$, temos pela definição 2.24

$$l^2\equiv -1 \bmod p\ ,\ \text{ onde } l\in\mathbb{Z}. \tag{2.1}$$

Considere o subconjunto M do $\mathbb{R}^2$ dado por

$$M=\mathbb{Z}\cdot v_1+\mathbb{Z}\cdot v_2\ ,\ \text{ onde } v_1=(1,l) \text{ e } v_2=(0,p)$$

Pelo ítem a) do lema 2.11, obtemos:

$$Vol(T_v)=\left|\det\begin{pmatrix} 1 & l \\ 0 & p \end{pmatrix}\right|=p\neq 0$$

Pelo lema 2.12 e a definição 2.16 segue que M é um reticulado com base $\{(1,l),(0,p)\}$ e

$$Vol(M)=Vol(T_v)=p.$$

Seja C a bola de centro zero e raio r do $\mathbb{R}^2$, ou seja

$$C = B_2(r) = \{(x, y) \in \mathbb{R}^2 \ ; \ x^2 + y^2 \leq r^2 \ \text{ onde } \ r \in \mathbb{R}_+^*\}$$

Pelo exemplo 2.21, C é convexo e centralmente simétrico e

$$Vol(C) = \pi \cdot r^2.$$

Fixando $r^2 = 1,28p$, temos:

$$Vol(C) = \pi \cdot r^2 \cong (3,14) \cdot (1,28) \cdot p = (4,0192) \cdot p > 4 \cdot p = 2^2 \cdot Vol(M).$$

Pelo teorema de Minkowski(corolário 2.23), $C \cap (M \setminus \{0\}) \neq \varnothing$.

Seja,

$$Q = m \cdot (1, l) + n \cdot (0, p) \ \text{ com } \ m, n \in \mathbb{Z}$$

um ponto de M no interior de C. Fazendo,

$$x = m \ \text{ e } \ y = lm + np \ ,$$

temos:

$$\begin{aligned} x^2 + y^2 &= m^2 + (lm + np)^2 = m^2 + l^2m^2 + 2lmnp + n^2p^2 \\ &= (1 + l^2)m^2 + (2lmn + n^2p)p. \end{aligned}$$

Então,

$$x^2 + y^2 \equiv (1 + l^2)m^2 \bmod p \tag{2.2}$$

Mas, por (2.1),

$$l^2 \equiv -1 \bmod p \implies 1 + l^2 = kp \implies (1 + l^2)m^2 = m^2kp \ ,$$

ou seja

$$(1 + l^2)m^2 \equiv 0 \bmod p \tag{2.3}$$

De (2.2) e (2.3),obtemos:

$$x^2 + y^2 \equiv 0 \bmod p \tag{2.4}$$

Por outro lado, como Q está no interior de C, então

$$0 < x^2 + y^2 < r^2 = 1,28p < 2p \tag{2.5}$$

Logo, de (2.4) e (2.5), x e y são inteiros que satisfazem $x^2 + y^2 = p$. ■

2.4 Soma de Quatro Quadrados

Nesta seção veremos mais alguns resultados necessários para a utilização do método geométrico, dentre eles, citamos o cálculo de volumes de bolas no $\mathbb{R}^n$, que será aqui apresentado de forma genérica. Para finalizarmos, apresentamos uma prova alternativa do teorema de Lagrange, utilizando o referido método.

Lema 2.30 *Para todo primo racional p, existem racionais inteiros x e y tais que $x^2 + y^2 + 1 \equiv 0(\mathrm{mod}\, p)$.*

Demonstração. Se -1 é um resto quadrático de p, então existe $a \in \mathbb{Z}$ tal que:

$$a^2 \equiv -1(\mathrm{mod}\, p) \implies a^2 + 1 \equiv 0(\mathrm{mod}\, p).$$

Então, fazendo $x = a$ e $y = 0$, temos

$$x^2 + y^2 + 1 = a^2 + 1 \equiv 0(\mathrm{mod}\, p).$$

Suponha que -1 não é um resto quadrático módulo p. Considere o conjunto:

$$S = \left\{y^2 + 1 \ ; \ y \in \mathbb{Z}\right\}$$

Pelo lema 2.26 existe $y \in \mathbb{Z}$ tal que $y^2 + 1 = z \in S$ não é um quadrado módulo p. Então, pelo lema 2.27 $-1 \cdot (y^2 + 1) = -y^2 - 1$ é um resto quadrático módulo p. Daí, existe um racional inteiro x tal que:

$$x^2 \equiv -y^2 - 1(\mathrm{mod}\, p)$$

Portanto, $x^2 + y^2 + 1 \equiv 0(\mathrm{mod}\, p)$. ■

Veremos a seguir informações sobre o volume de bolas de raio r no $\mathbb{R}^n$, que é crucial para a aplicação da técnica do limite convexo de Minkowski.

Lema 2.31 *Seja $B_m(r)$ a bola fechada de raio r, em $\mathbb{R}^m$, centrada na origem. Seu volume Euclideano é:*

$$Vol\left(B_{2n}(r)\right) = \frac{\pi^n}{n!} \cdot r^{2n} \quad , \quad Vol\left(B_{2n-1}(r)\right) = \frac{2^n \cdot \pi^{n-1}}{1 \times 3 \times \cdots \times (2n-1)} \cdot r^{2n-1}.$$

Demonstração. Para simplificarmos a notação utilizaremos $V_n(r)$ para representar a bola do $\mathbb{R}^n$ de raio r, centrada na origem. Pela definição de volume no $\mathbb{R}^n$, temos:

$$V_{n+1}(r) = \int_{\mathbb{R}^{n+1}} \chi(w) dw \ ,$$

onde $\chi : \mathbb{R}^{n+1} \longrightarrow \mathbb{R}$ é a função característica de $V_{n+1}(r)$.

Pelo teorema da integração repetida, temos que:

$$V_{n+1}(r) = 2 \cdot \int_0^r \left(\int_{\mathbb{R}^n} \chi_t(x)dx \right) dt \ ,$$

onde χ_t é a função característica do seguinte conjunto:

$$\{x \in \mathbb{R}^n \ ; \ t \geq 0 \ , \ (x,t) \in B_{n+1}(r)\} = B_n\left(te_j, \sqrt{r^2 - t^2}\right),$$

então:

$$\begin{aligned} \int_{\mathbb{R}^n} \chi_t(x)dx &= Vol\left(B_n\left(te_j, \sqrt{r^2 - t^2}\right)\right) = V_n\left(\sqrt{r^2 - t^2}\right) \\ &= \left(\sqrt{r^2 - t^2}\right) \cdot V_n(1), \end{aligned}$$

em virtude do ítem c) do lema 2.11. Daí,

$$V_{n+1}(r) = 2 \cdot \int_0^r V_n(1) \cdot (r^2 - t^2)^{\frac{n}{2}} dt \ , \tag{2.6}$$

onde $0 \leq t \leq r$ ou $0 \leq \frac{t}{r} \leq 1$. Fazendo $sen(x) = \frac{t}{r}$, temos:

$$0 \leq x \leq \frac{\pi}{2} \ \text{ e } \ dt = r \cdot \cos(x)dx.$$

Pela 1^a relação fundamental da trigonometria, temos:

$$\left(\frac{t}{r}\right)^2 + \cos^2(x) = 1 \implies \cos^2(x) = 1 - \frac{t^2}{r^2} = \frac{r^2 - t^2}{r^2},$$

e segue que

$$\cos(x) = \frac{1}{r} \cdot \sqrt{r^2 - t^2} \implies \cos^n(x) = \frac{1}{r^n} \cdot \left(\sqrt{r^2 - t^2}\right)^n,$$

donde

$$\left(\sqrt{r^2 - t^2}\right)^n = r^n \cdot \cos^n(x).$$

Portanto,

$$\int_0^r \left(\sqrt{r^2 - t^2}\right)^n dt = \int_0^{\frac{\pi}{2}} r^n \cdot \cos^n(x) \cdot r \cdot \cos(x)dx = r^{n+1} \cdot \int_0^{\frac{\pi}{2}} \cos^{n+1}(x)dx.$$

Utilizaremos agora a seguinte fórmula:

$$\int \cos^n(x)dx = \frac{\cos^{n-1}(x) \cdot sen(x)}{n} + \frac{n-1}{n} \cdot \int \cos^{n-2}(x)dx.$$

Então,

$$\begin{aligned}\int_0^r \left(r^2-t^2\right)^{\frac{n}{2}}dt &= r^{n+1}\cdot\left(\underbrace{\frac{\cos^n(x)\cdot sen(x)}{n+1}\Big|_0^{\frac{\pi}{2}}}_{=0}+\frac{n}{n+1}\cdot\int_0^{\frac{\pi}{2}}\cos^{n-1}(x)dx\right)\\ &= r^{n+1}\cdot\frac{n}{n+1}\cdot\int_0^{\frac{\pi}{2}}\cos^{n-1}(x)dx.\end{aligned}$$

Assim, aplicando a fórmula n-vezes, temos:

$$\int_0^r \left(r^2-t^2\right)^{\frac{n}{2}}dt=\begin{cases} r^{n+1}\cdot\frac{n}{n+1}\cdot\frac{n-2}{n-1}\cdot\frac{n-4}{n-3}\cdot\cdots\cdot 1, \text{ se } n \text{ for par}\\ \\ r^{n+1}\cdot\frac{n}{n+1}\cdot\frac{n-2}{n-1}\cdot\frac{n-4}{n-3}\cdot\cdots\cdot 1\cdot\frac{\pi}{2}, \text{ se } n \text{ for ímpar}\end{cases}$$

Voltando a (2.6), temos:

$$V_{n+1}(r)=2\cdot r^{n+1}\cdot V_n(1)\cdot\begin{cases} r^{n+1}\cdot\frac{n}{n+1}\cdot\frac{n-2}{n-1}\cdot\frac{n-4}{n-3}\cdot\cdots\cdot 1, \text{ se } n+1 \text{ é ímpar}\\ \\ r^{n+1}\cdot\frac{n}{n+1}\cdot\frac{n-2}{n-1}\cdot\frac{n-4}{n-3}\cdot\cdots\cdot 1\cdot\frac{\pi}{2}, \text{ se } n+1 \text{ é par}\end{cases}$$

Pelo que foi feito anteriormente, temos que:

$$V_n(1)=2\cdot V_{n-1}(1)\cdot\begin{cases}\frac{n-1}{n}\cdot\frac{n-3}{n-2}\cdot\frac{n-5}{n-4}\cdot\cdots\cdot 1\cdot\frac{\pi}{2}\ ,\ n\text{-par}\\ \\ \frac{n-1}{n}\cdot\frac{n-3}{n-2}\cdot\frac{n-5}{n-4}\cdot\cdots\cdot 1\ ,\ n\text{-ímpar}\end{cases}$$

e

$$V_{n-1}(1)=2\cdot V_{n-2}(1)\cdot\begin{cases}\frac{n-2}{n-1}\cdot\frac{n-4}{n-3}\cdot\frac{n-6}{n-5}\cdot\cdots\cdot 1\ ,n\text{-par}\\ \\ \frac{n-2}{n-1}\cdot\frac{n-4}{n-3}\cdot\frac{n-6}{n-5}\cdot\cdots\cdot 1\cdot\frac{\pi}{2}\ ,n\text{-ímpar}\end{cases}$$

Continuando este processo, podemos expressar $V_{n+1}(r)$ pela fórmula abaixo:

$$V_{n+1}(r)=\begin{cases}\underbrace{2^{n+1}\cdot r^{n+1}\cdot\left(\frac{n}{n+1}\cdot\frac{n-2}{n-1}\cdot\cdots\cdot 1\right)\cdot\left(\frac{n-1}{n}\cdot\frac{n-3}{n-2}\cdot\cdots\cdot 1\cdot\frac{\pi}{2}\right)\cdot\cdots\cdot 1\cdot\frac{\pi}{2}}_{\text{Produto de } n \text{ fatores, com } n+1 \text{ ímpar}}\\ \\ \underbrace{2^{n+1}\cdot r^{n+1}\cdot\left(\frac{n}{n+1}\cdot\frac{n-2}{n-1}\cdot\cdots\cdot 1\cdot\frac{\pi}{2}\right)\cdot\left(\frac{n-1}{n}\cdot\frac{n-3}{n-2}\cdot\cdots\cdot 1\right)\cdot\cdots\cdot 1\cdot\frac{\pi}{2}}_{\text{Produto de } n \text{ fatores, com } n+1 \text{ par}}\end{cases}$$

e, simplificando, obtemos:

$$
\begin{aligned}
V_{n+1}(r) &= 2^{n+1}\cdot r^{n+1}\cdot \begin{cases} \frac{\pi^{\frac{n}{2}}}{2^{\frac{n}{2}}}\cdot\frac{\left(\frac{n}{2}\cdot 2\right)\cdot\left(\frac{n-2}{2}\cdot 2\right)\cdot\left(\frac{n-4}{2}\cdot 2\right)\cdot\cdots\cdot 1}{(n+1)\cdot n\cdot(n-1)\cdot(n-2)\cdot\cdots\cdot 1}\ , & (n+1)\text{-ímpar} \\ \\ \frac{\pi^{\frac{n+1}{2}}}{2^{\frac{n+1}{2}}}\cdot\frac{1}{\left(\frac{n+1}{2}\right)\cdot 2\cdot\left(\frac{n-1}{2}\right)\cdot 2\cdot\left(\frac{n-3}{2}\right)\cdot 2\cdot\cdots\cdot 1\cdot 2}\ , & (n+1)\text{-par} \end{cases} \\
&= 2^{n+1}\cdot r^{n+1}\cdot \begin{cases} \frac{\pi^{\frac{n}{2}}}{2^{\frac{n}{2}}}\cdot\frac{2^{\frac{n}{2}}\cdot\left(\frac{n}{2}\right)!}{(n+1)!}\ , & (n+1)\text{-ímpar} \\ \\ \frac{\pi^{\frac{n+1}{2}}}{2^{\frac{n+1}{2}}}\cdot\frac{1}{2^{\frac{n+1}{2}}\cdot\left(\frac{n+1}{2}\right)!}\ , & (n+1)\text{-par} \end{cases} \\
&= \begin{cases} 2^{n+1}\cdot r^{n+1}\cdot\pi^{\frac{n}{2}}\cdot\frac{\left(\frac{n}{2}\right)!}{(n+1)!}\ , & (n+1)\text{-ímpar} \\ \\ r^{n+1}\cdot\pi^{\frac{n+1}{2}}\cdot\frac{1}{\left(\frac{n+1}{2}\right)!}\ , & (n+1)\text{-par} \end{cases}
\end{aligned}
$$

Portanto, o resultado segue. ■

Vamos agora provar o principal resultado desta seção pela técnica do limite convexo.

Teorema 2.32 *Todo inteiro positivo é soma de quatro quadrados de inteiros racionais.*

Demonstração. Por argumentos vistos no teorema 1.20, basta provarmos o teorema para os primos racionais. Dado um primo p, pelo lema 2.30, existem inteiros a e b tais que

$$a^2 + b^2 + 1 \equiv 0 (\mathrm{mod}\, p). \tag{2.7}$$

Considere o subconjunto M do $\mathbb{R}^4$ dado por:

$$M = \mathbb{Z}\cdot v_1 + \mathbb{Z}\cdot v_2 + \mathbb{Z}\cdot v_3 + \mathbb{Z}\cdot v_4\ ,$$

onde

$$v_1 = (1,0,a,b)\ ,\ v_2 = (0,1,b,-a)\ ,\ v_3 = (0,0,p,0)\ ,\ v_4 = (0,0,0,p).$$

Do lema 2.11, obtemos:

$$Vol(T_v) = \left|\det\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & b & -a \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}\right| = |1\cdot 1\cdot p\cdot p| = p^2 \neq 0.$$

Em virtude do lema 2.12 e a definição 2.16, M é um reticulado com base $\{v_1, v_2, v_3, v_4\}$ e

$$Vol(M) = Vol(T_v) = p^2.$$

Um ponto qualquer deste reticulado é dado por:

$$x \cdot (1,0,a,b) + y \cdot (0,1,b,-a) + k \cdot (0,0,p,0) + m \cdot (0,0,0,p) =$$
$$= (x, y, ax + by + kp, bx - ay + mp), \text{ com } x, y, k, m \in \mathbb{Z}.$$

Fazendo,

$$z = ax + by + kp \text{ e } w = bx - ay + mp \ ,$$

temos que um elemento típico deste reticulado é da forma (x, y, z, w), $x, y, z, w \in \mathbb{Z}$ tais que:

$$\begin{cases} z \equiv ax + by (\mathrm{mod}\, p) \\ w \equiv bx - ay (\mathrm{mod}\, p) \end{cases} \tag{2.8}$$

Seja $B_4(r)$ a bola de raio r centrada na origem em $\mathbb{R}^4$. Pelo lema 2.31, temos que:

$$Vol(B_4(r)) = \frac{\pi^2}{2!} \cdot r^4 = \frac{\pi^2}{2} \cdot r^4$$

Fazendo $r^2 = 1,81p$, temos:

$$\begin{aligned} Vol(B_4(r)) &= \frac{\pi^2}{2} \cdot \left(r^2\right)^2 \cong \frac{(3,14)^2}{2} \cdot (1,81p)^2 = \\ &= \frac{9,8596}{2} \cdot (3,2761) \cdot p^2 = (4,9298) \cdot (3,2761) \cdot p^2 = \\ &= (16,150518) \cdot p^2 > 16 \cdot p^2 = 2^4 \cdot Vol(M) \end{aligned}$$

Daí, algum r tal que $r^2 > 1,81p$ será suficiente. Escolhendo r tal que $r^2 = 1,9p$ e observando pelo teorema 2.22 que $B_4(r)$ é convexa e centralmente simétrica então, pelo teorema de Minkowski(corolário 2.23) temos $B_4(r) \cap (M \setminus \{0\}) \neq \varnothing$.

Seja $(x, y, z, w) \in M$ um ponto no interior de $B_4(r)$, ou seja:

$$\|(x, y, z, w)\| \leq r \implies \sqrt{x^2 + y^2 + z^2 + w^2} \leq r,$$

ou seja,

$$x^2 + y^2 + z^2 + w^2 \leq r^2 = 1,9p \tag{2.9}$$

Mas, para esta escolha de inteiros x, y, z e w, temos por (2.7) e (2.8) que:

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 &\equiv (x^2 + y^2 + a^2x^2 + 2abxy + b^2y^2 + b^2x^2 - 2abxy + a^2y^2) \bmod p \\ &\equiv (x^2(1 + a^2 + b^2) + y^2(1 + a^2 + b^2)) \bmod p \\ &\equiv [(x^2 + y^2)(1 + a^2 + b^2)] \bmod p \\ &\equiv 0 \bmod p. \end{aligned}$$

Portanto,

$$p \,|(x^2 + y^2 + z^2 + w^2)$$

e por (2.9), concluimos que $p = x^2 + y^2 + z^2 + w^2$. ■

Capítulo 3

Teorema dos Quatro Quadrados de Götzky

Neste capítulo trataremos do principal resultado do nosso trabalho, ou seja, apresentaremos uma prova alternativa do Teorema dos quatro quadrados de Götzky utilizando resultados da geometria de números. Para tanto, estudaremos inicialmente os corpos quadráticos e, em particular, o corpo $\mathbb{Q}(\sqrt{5})$.

3.1 Corpos Quadráticos

Nesta seção estudaremos os corpos quadráticos e mostraremos que todo corpo quadrático possui um elemento primitivo distinguido da forma $\sqrt{d}$, univocamente determinado a menos do sinal, onde d é um número inteiro "livre de quadrados".

Definição 3.1 *Um subcorpo L de $\mathbb{C}$ é dito um corpo quadrático se $[L:\mathbb{Q}]=2$.*

Lema 3.2 *Qualquer $\alpha \in L \setminus \mathbb{Q}$ é um elemento primitivo da extensão $L \mid \mathbb{Q}$.*

Demonstração. De fato, observe que:

$$1 < [\mathbb{Q}(\alpha):\mathbb{Q}] \leq [L:\mathbb{Q}] = 2;$$

portanto, $\mathbb{Q}(\alpha) = L$. ■

Observação 3.3 *Os elementos $1, \alpha$ formam uma base desta extensão e, $p_{\alpha|\mathbb{Q}} = f_{\alpha,L|\mathbb{Q}}$ é um polinômio em $\mathbb{Q}[x]$ de grau 2.*

Considere o seguinte conjunto:

$$\mathfrak{D} = \{d \in \mathbb{Z} \setminus \{0,1\} : c^2 \nmid d, \text{ onde } c \in \mathbb{Z} \text{ e } c^2 \neq 1\}.$$

Proposição 3.4 *A aplicação definida por* $d \longmapsto \mathbb{Q}(\sqrt{d})$ *é uma bijeção de* $\mathfrak{D}$ *sobre o conjunto de todos os corpos quadráticos.*

Demonstração. Para qualquer $d \in \mathfrak{D}$ temos que $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}] \leq 2$, pois $p_{\sqrt{d}|\mathbb{Q}}$ divide $x^2 - d$. Vale a igualdade, pois caso contrário teríamos:

$$\sqrt{d} \in \mathbb{Q} \implies \sqrt{d} \in \mathbb{Z} \implies d = (\sqrt{d})^2 \notin \mathfrak{D} \text{ (Absurdo!)}.$$

Para provar que a aplicação é injetiva, supomos que:

$$\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'}), \text{ onde } d, d' \in \mathfrak{D}.$$

Daí, existem $r, s \in \mathbb{Q}$ tais que:

$$\sqrt{d'} = r + s \cdot \sqrt{d} \implies d' = r^2 + s^2 \cdot d + 2 \cdot r \cdot s \cdot \sqrt{d}.$$

Como $d' \in \mathbb{Z}$, temos:

$$r \cdot s = 0 \implies r = 0 \text{ ou } s = 0.$$

Se $s = 0$, então,

$$\sqrt{d'} = r \in I_L \cap \mathbb{Q} = \mathbb{Z} \implies d' \notin \mathfrak{D} \text{ (Absurdo!)}.$$

Portanto,

$$r = 0 \text{ e } d' = s^2 \cdot d.$$

Nas fatorações de d' e de d, todo número primo p ocorre com um expoente 0 ou 1; na fatoração de s^2, porém, com um expoente par; donde resulta que:

$$s^2 = 1 \implies d' = d.$$

Seja $L = \mathbb{Q}(\alpha)$ um corpo quadrático com,

$$p_{\alpha|\mathbb{Q}} = x^2 + a \cdot x + b \in \mathbb{Q}[x].$$

Pondo $\beta = \alpha + \frac{a}{2}$, temos:

$$L = \mathbb{Q}(\beta) \text{ e } p_{\beta|\mathbb{Q}} = x^2 - \left(\frac{a^2}{4} - b\right).$$

Vê-se facilmente que existem $d \in \mathfrak{D}$ e $r \in \mathbb{Q} \setminus \{0\}$ tais que:

$$\frac{a^2}{4} - b = r^2 \cdot d \ ;$$

obviamente $L = \mathbb{Q}(\sqrt{d})$. ■

Usando $1, \sqrt{d}$ como base da extensão $L = \mathbb{Q}(\sqrt{d})$ de $\mathbb{Q}$, o polinômio característico de qualquer elemento $\alpha = r + s \cdot \sqrt{d} \in L$ é obtido, como:

$$f_{\alpha, L|\mathbb{Q}} = \begin{vmatrix} x - r & -s \\ -s \cdot d & x - r \end{vmatrix} = x^2 - 2 \cdot r \cdot x + r^2 - s^2 \cdot d \ ,$$

uma vez que $\alpha \cdot 1 = r + s \cdot \sqrt{d}$ e $\alpha \cdot \sqrt{d} = s \cdot d + r \cdot \sqrt{d}$. Portanto, temos que:

$$\mathcal{T}_{L|\mathbb{Q}}(\alpha) = 2 \cdot r \ \text{ e } \ \mathcal{N}_{L|\mathbb{Q}}(\alpha) = r^2 - s^2 \cdot d. \tag{3.1}$$

Proposição 3.5 *Seja $L = \mathbb{Q}(\sqrt{d})$, onde $d \in \mathfrak{D}$. Então:*

$$I_L = \left\{ \frac{m}{2} + \frac{n}{2} \cdot \sqrt{d} : m, n \in \mathbb{Z} \ ; \ m^2 \equiv n^2 \cdot d (\mathrm{mod}\, 4) \right\}$$

Demonstração. $\supseteq$: Se,

$$\alpha = \frac{m}{2} + \frac{n}{2} \cdot \sqrt{d} \ \text{ com } \ m, n \in \mathbb{Z} \ \text{ e } \ m^2 \equiv n^2 \cdot d (\mathrm{mod}\, 4),$$

então:

$$f_{\alpha, L|\mathbb{Q}} = x^2 - 2 \cdot \frac{m}{2} \cdot x + \frac{m^2}{4} - \frac{n^2}{4} \cdot d = x^2 - m \cdot x + \frac{m^2 - n^2 \cdot d}{4}.$$

Como $m^2 \equiv n^2 \cdot d (\mathrm{mod}\, 4)$ temos que $f_{\alpha, L|\mathbb{Q}} \in \mathbb{Z}[x]$; logo $\alpha \in I_L$.

$\subseteq$: Sejam $r, s \in \mathbb{Q}$ tais que $\alpha = r + s \cdot \sqrt{d} \in I_L$; então:

$$2 \cdot r = \mathcal{T}_{L|\mathbb{Q}}(\alpha) \in \mathbb{Z} \ \text{ e } \ r^2 - s^2 \cdot d = \mathcal{N}_{L|\mathbb{Q}}(\alpha) \in \mathbb{Z} \ ;$$

logo,

$$(2 \cdot s)^2 \cdot d = (2 \cdot r)^2 - 4 \cdot (r^2 - s^2 \cdot d) \in \mathbb{Z}.$$

Sendo $k_p \in \mathbb{Z}$ (respectivamente $e_p \in \{0, 1\}$), o expoente do número primo p na fatoração de $2 \cdot s$ (respectivamente de d), concluímos que:

$$2 \cdot k_p + e_p \geq 0 \implies k_p \geq 0 \implies 2 \cdot s \in \mathbb{Z}.$$

Chamando de $m = 2 \cdot r$ e $n = 2 \cdot s$, então $r = \frac{m}{2}$ e $s = \frac{n}{2}$. Daí,

$$\alpha = \frac{m}{2} + \frac{n}{2} \cdot \sqrt{d} \ \text{ e que } \ m^2 - n^2 \cdot d = 4 \cdot r^2 - 4 \cdot s^2 \cdot d = 4 \cdot (r^2 - s^2 \cdot d)$$

é um múltiplo de 4. ■

Teorema 3.6 *Seja* $L = \mathbb{Q}(\sqrt{d})$ *onde* $d \in \mathfrak{D}$, *e seja* $\delta = \sqrt{d}$ $\left(\textit{respectivamente} = \frac{1+\sqrt{d}}{2}\right)$ *no caso em que* $d \equiv 2$ *ou* 3 *(respectivamente* $\equiv 1$*)* $\bmod 4$. *Então,* $1, \delta$ *formam uma base do* $\mathbb{Z}$ *- módulo* I_L.

Demonstração. Os elementos $1, \delta$ são linearmente independentes sobre $\mathbb{Z}$, pois o são sobre $\mathbb{Q}$; por isto, basta provar que $\mathbb{Z} + \mathbb{Z} \cdot \delta = I_L$. Se,

1^o) $\delta = \sqrt{d}$, com $d \equiv 2$ ou $3 \bmod 4$, temos:

$$\delta = \frac{0}{2} + \frac{2}{2} \cdot \sqrt{d} \text{ e } 0^2 \equiv 2^2 \cdot d \bmod 4.$$

2^o) $\delta = \frac{1}{2} + \frac{1}{2} \cdot \sqrt{d}$, com $d \equiv 1 \bmod 4$, temos:

$$m = 1, n = 1 \text{ e } m^2 = 1 \equiv d = n^2 \cdot d \bmod 4.$$

Portanto, $\delta \in I_L$ e $\mathbb{Z} + \mathbb{Z} \cdot \delta \subseteq I_L$. Para provar a inclusão inversa, observamos pela proposição 3.5, que qualquer $\alpha \in I_L$ é da forma:

$$\frac{m}{2} + \frac{n}{2} \cdot \sqrt{d}, \text{ com } m, n \in \mathbb{Z} \text{ e } m^2 \equiv n^2 \cdot d (\bmod 4).$$

No caso em que $d \equiv 1 \bmod 4$, temos que:

$$m^2 \equiv n^2 \cdot (1 + 4 \cdot k) \bmod 4 \implies m^2 \equiv n^2 \bmod 4.$$

Daí, m e n possuem a mesma paridade, digamos $m = 2k + n$ com $k \in \mathbb{Z}$. Logo:

$$\alpha = \frac{2k+n}{2} + \frac{n}{2} \cdot \sqrt{d} = k + n \cdot \left(\frac{1+\sqrt{d}}{2}\right) = k + n \cdot \delta.$$

No caso em que $d \equiv 2$ ou $3 \bmod 4$, basta mostrar que m e n são pares. Se n fosse ímpar teríamos:

$$n^2 \equiv 1 \bmod 4 \implies n^2 = 1 + 4t \implies m^2 \equiv (1 + 4t) \cdot d \bmod 4 \implies m^2 \equiv d \bmod 4 \ ;$$

e, portanto, $d \equiv 0$ ou $\equiv 1 \bmod 4$ (Absurdo!). Concluímos que n é par, e de $m^2 \equiv n^2 \cdot d \equiv 0 \bmod 4$ decorre que m também é par. ■

Pretendemos agora tratarmos de corpos quadráticos L para os quais I_L seja um domínio fatorial e, para tanto, usaremos a noção de domínio euclidiano.

Definição 3.7 *Diremos que um domínio R é* euclidiano *se existir uma aplicação $\partial : R \setminus \{0\} \longrightarrow \mathbb{N}$ com as seguintes propriedades: Para quaisquer $a, b \in R \setminus \{0\}$,*

(i) *de $a \mid b$ decorre $\partial(a) \leq \partial(b)$.*

(ii) *existem $q, r \in R$ tais que $a = q \cdot b + r$ e $[r = 0$ ou $\partial(r) < \partial(b)]$.*

Proposição 3.8 *Todo domínio euclidiano é principal e, portanto, fatorial.*

Demonstração. Dado um ideal não-nulo $\mathfrak{a}$ de R, existe $b \in \mathfrak{a} \setminus \{0\}$ tal que $\partial(b)$ seja minimal em $\{\partial(a) : a \in \mathfrak{a} \setminus \{0\}\}$. Para qualquer $a \in \mathfrak{a}$ sejam $q, r \in R$ tais que:

$$a = q \cdot b + r \text{ e } [r = 0 \text{ ou } \partial(r) < \partial(b)].$$

Como $r = a - q \cdot b \in \mathfrak{a}$, a desigualdade $\partial(r) < \partial(b)$ é impossível devido à minimalidade de $\partial(b)$; portanto,

$$r = 0 \text{ e } a = q \cdot b \in (b) \implies \mathfrak{a} = (b).$$

Resulta que R é um domínio principal, logo fatorial. ■

Observação 3.9 *No caso do anel I_L dos inteiros algébricos de um corpo quadrático $L = \mathbb{Q}(\sqrt{d})$, um candidato natural para a aplicação ∂ é a norma absoluta (restrita a $I_L \setminus \{0\}$), isto é, a aplicação definida por $\alpha \longmapsto \left|\mathcal{N}_{L|\mathbb{Q}}(\alpha)\right|$.*

Proposição 3.10 *Dado $\gamma \in \mathbb{Q}(\sqrt{5})$, existe $k \in I_{\mathbb{Q}(\sqrt{5})}$ tal que $\left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma - k)\right| < 1$.*

Demonstração. Sejam

$$\gamma = r + s\sqrt{5} \text{ e } k = x + y\left(\frac{1+\sqrt{5}}{2}\right), \text{ com } r, s \in \mathbb{Q} \text{ e } x, y \in \mathbb{Z};$$

daí,

$$\gamma - k = r - x - \frac{y}{2} + \left(s - \frac{y}{2}\right) \cdot \sqrt{5}.$$

Por (3.1), temos:

$$\begin{aligned} \left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma - k)\right| &= \left|\left(r - x - \frac{y}{2}\right)^2 - 5 \cdot \left(s - \frac{y}{2}\right)^2\right| \\ &= \left|\left(r - x - \frac{y}{2}\right)^2 - \frac{5}{4} \cdot (2s - y)^2\right|; \end{aligned}$$

e portanto,

$$\left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma - k)\right| < 1 \iff \left|\left(r - x - \frac{y}{2}\right)^2 - \frac{5}{4} \cdot (2s - y)^2\right| < 1 \qquad (3.2)$$

Suponha que (3.2) é falsa para alguns racionais r, s e todos os inteiros x, y ; e nós podemos supor que:

$$0 \leq r \leq \frac{1}{2} \text{ e } 0 \leq 2s \leq \frac{1}{2}. \tag{3.3}$$

Existe daí um par em (3.3), tais que uma das desigualdades abaixo é satisfeita:

$$[P(x,y)] : \left(r - x - \tfrac{y}{2}\right)^2 \geq 1 + \tfrac{5}{4} \cdot (2s - y)^2 ,$$
$$[N(x,y)] : \tfrac{5}{4} \cdot (2s - y)^2 \geq 1 + \left(r - x - \tfrac{y}{2}\right)^2 .$$

Em particular, vamos fazer uso das desigualdades:

$$[P(0,0)] : r^2 \geq 1 + 5s^2 \ , \qquad [N(0,0)] : 5s^2 \geq 1 + r^2$$
$$[P(1,0)] : (1-r)^2 \geq 1 + 5s^2 \ , \qquad [N(1,0)] : 5s^2 \geq 1 + (1-r)^2$$
$$[P(-1,0)] : (1+r)^2 \geq 1 + 5s^2 \ , \qquad [N(-1,0)] : 5s^2 \geq 1 + (1+r)^2$$

Se $r = s = 0$, então $P(0,0)$ e $N(0,0)$ são ambas falsas, o que é impossível. Se r e $2s$ satisfazem (3.3) e não são ambos nulos então, $P(0,0)$ e $P(1,0)$ são falsas; e daí $N(0,0)$ e $N(1,0)$ são verdadeiras.

Se $P(-1,0)$ é verdadeira, então $N(1,0)$ e $P(-1,0)$ nos dará:

$$(1+r)^2 \geq 1 + 5s^2 \geq 2 + (1-r)^2;$$

donde resulta que:

$$1 + 2r + r^2 \geq 2 + 1 - 2r + r^2 \implies 4r \geq 2 \implies r \geq \frac{1}{2};$$

e por (3.3), temos:

$$r = \frac{1}{2} \implies 5s^2 \geq 1 + \frac{1}{4} \implies 5s^2 \geq \frac{5}{4};$$

ou seja, $s^2 \geq \frac{1}{4}$ (absurdo!).

Daí, $P(-1,0)$ é falsa, e então $N(-1,0)$ é verdadeira. Portanto,

$$5s^2 \geq 1 + (1+r)^2 = 2 + 2r + r^2 \geq 2 \text{ (absurdo!)}.$$

Logo, a proposição segue. ■

Corolário 3.11 *$I_{\mathbb{Q}(\sqrt{5})}$ é euclidiano com relação à norma absoluta.*

Demonstração. Sejam $\delta, \gamma_1 \in I_{\mathbb{Q}(\sqrt{5})}$ com $\gamma_1 \neq 0$. Temos que $\frac{\delta}{\gamma_1} \in \mathbb{Q}(\sqrt{5})$ e, pela proposição 3.10, existe $k \in I_{\mathbb{Q}(\sqrt{5})}$ tal que:

$$\left| \mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}} \left(\frac{\delta}{\gamma_1} - k \right) \right| < 1. \tag{3.4}$$

Tomando $\gamma_2 = \delta - k \cdot \gamma_1 \in I_{\mathbb{Q}(\sqrt{5})}$, temos:

$$\delta = k \cdot \gamma_1 + \gamma_2,$$

e

$$\begin{aligned} \left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma_2)\right| &= \left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}\left[\gamma_1 \cdot \left(\frac{\delta}{\gamma_1} - k\right)\right]\right| \\ &= \left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma_1)\right| \cdot \left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}\left(\frac{\delta}{\gamma_1} - k\right)\right|; \end{aligned}$$

e por (3.4), temos $\left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma_2)\right| < \left|\mathcal{N}_{\mathbb{Q}(\sqrt{5})|\mathbb{Q}}(\gamma_1)\right|$. ■

Veremos agora o discriminante para corpos quadráticos, dado na seguinte proposição:

Proposição 3.12 *Seja $L = \mathbb{Q}(\sqrt{d})$, sendo $d \in \mathfrak{D}$. Então:*

$$d_L = \begin{cases} 4d \ \textit{quando} \ d \equiv 2 \ \textit{ou} \ 3 \bmod 4 \\ d \ \textit{quando} \ d \equiv 1 \bmod 4 \end{cases}$$

Demonstração. Para qualquer $\alpha = r + s \cdot \sqrt{d}$, com $r, s \in \mathbb{Q}$, temos que:

$$\alpha^2 = (r^2 + s^2 \cdot d) + 2 \cdot r \cdot s \cdot \sqrt{d}\ ;$$

logo,

$$\begin{aligned} disc_{L|\mathbb{Q}}(1, \alpha) &= \det \begin{pmatrix} \mathcal{T}_{L|\mathbb{Q}}(1) & \mathcal{T}_{L|\mathbb{Q}}(\alpha) \\ \mathcal{T}_{L|\mathbb{Q}}(\alpha) & \mathcal{T}_{L|\mathbb{Q}}(\alpha^2) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 2 \cdot r \\ 2 \cdot r & 2 \cdot (r^2 + s^2 \cdot d) \end{pmatrix} = 4 \cdot s^2 \cdot d. \end{aligned}$$

Em particular, temos que:

$$disc_{L|\mathbb{Q}}(1, \sqrt{d}) = 4 \cdot d \ \text{ e } \ disc_{L|\mathbb{Q}}\left(1, \frac{1 + \sqrt{d}}{2}\right) = d.$$

Como, pelo teorema 3.6, $1, \sqrt{d}$ $\left(\text{respectivamente } 1, \frac{1+\sqrt{d}}{2}\right)$ formam uma base integral de L no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) $\bmod 4$, obtemos o resultado desejado. ■

Apresentaremos agora as unidades e os primos de $I_{\mathbb{Q}(\sqrt{5})}$.

Lema 3.13 *Seja $\omega = \frac{1+\sqrt{5}}{2}$. Não existe nenhuma unidade $\varepsilon \in U\left(I_{\mathbb{Q}(\sqrt{5})}\right)$ tal que $1 < \varepsilon < \omega$.*

Demonstração. Suponha que exista uma unidade $\varepsilon = a + b \cdot \left(\frac{1+\sqrt{5}}{2}\right)$ tal que:

$$\begin{gathered} 1 < a + b \cdot \left(\frac{1+\sqrt{5}}{2}\right) = \varepsilon < \omega = \frac{1+\sqrt{5}}{2} < 2 \\ a^2 + ab - b^2 = \pm 1 \ ; \end{gathered} \tag{3.5}$$

daí, temos:

$$-1 < a - b \cdot \left(\frac{1+\sqrt{5}}{2}\right) < 1. \tag{3.6}$$

De (3.5) e (3.6) obtemos:

$$0 < 2a < 1 + \frac{1+\sqrt{5}}{2} < 3 \implies 2a = 2 \implies a = 1,$$

pois $a \in \mathbb{Z}$; e portanto,

$$1 < 1 + b \cdot \left(\frac{1+\sqrt{5}}{2}\right) < \frac{1+\sqrt{5}}{2},$$

que é impossível para $b \in \mathbb{Z}$. ■

Teorema 3.14 *Seja $L = \mathbb{Q}(\sqrt{5})$. Então:*

$$U\left(I_{\mathbb{Q}(\sqrt{5})}\right) = \left\{ \pm\omega^{\pm n} : \omega = \frac{1+\sqrt{5}}{2} \ \ e \ n \in \mathbb{N} \right\}.$$

Demonstração. Temos que:

$$\mathcal{N}(\omega) = \mathcal{N}\left(\frac{1+\sqrt{5}}{2}\right) = \frac{1}{4} - 5 \cdot \frac{1}{4} = -1 \ ;$$

portanto, ω é uma unidade. Como $U\left(I_{\mathbb{Q}(\sqrt{5})}\right)$ é um grupo, então $\pm\omega^{\pm n}$ são unidades. Vamos mostrar que estas são as únicas unidades de $I_{\mathbb{Q}(\sqrt{5})}$. Seja $\varepsilon \in U\left(I_{\mathbb{Q}(\sqrt{5})}\right)$. Sem perda de generalidade podemos supor que $\varepsilon > 0$. Como $\varepsilon \in \mathbb{R}$ e $\mathbb{R}$ é arquimediano, temos:

$$\varepsilon = \omega^n \ \text{ ou } \ \omega^n < \varepsilon < \omega^{n+1} (n \in \mathbb{Z}).$$

Temos ainda que $\omega^{-n} \cdot \varepsilon$ é uma unidade e, admitindo o segundo caso, segue que:

$$\omega^{-n} \cdot \omega^n = 1 < \omega^{-n} \cdot \varepsilon < \omega^{-n} \cdot \omega^{n+1} = \omega \ ;$$

o que é um absurdo em virtude do lema 3.13. Portanto, $\varepsilon = \omega^n$. Desde que $-\varepsilon$ é uma unidade se ε é uma unidade, então o teorema segue. ■

Teorema 3.15 5 *é um resto quadrático dos primos racionais da forma* $10n \pm 1$ *e um não-resto quadrático dos primos racionais da forma* $10n \pm 3$. ■

Teorema 3.16 *Os primos de* $\mathbb{Q}(\sqrt{5})$ *são* $(1)\sqrt{5}$, (2) *os primos racionais* $5n \pm 2$, (3) *os fatores* $a + b\omega$ *dos primos racionais* $5n \pm 1$ *(e os associados destes números).*

Demonstração. Seja $\pi = a + b\omega$ um primo de $\mathbb{Q}(\sqrt{5})$. Em virtude do corolário A.17, a determinação destes primos depende da equação:

$$\mathcal{N}(\pi) = a^2 + ab - b^2 = p \ ;$$

ou seja:

$$4a^2 + 4ab + b^2 - 5b^2 = 4p \implies (2a + b)^2 - 5b^2 = 4p.$$

Se $p = 5n \pm 2$, então:

$$(2a + b)^2 - 5b^2 = 20n \pm 8 \implies (2a + b)^2 \equiv \pm 3 \bmod 5,$$

que é impossível. Daí estes primos são primos em $\mathbb{Q}(\sqrt{5})$.

Se $p = 5n \pm 1$, então pelo teorema 3.15 5 é resto quadrático $\bmod p$, ou seja:

$$p \mid (x^2 - 5) \text{ para algum } x \in \mathbb{Q}(\sqrt{5}),$$

e portanto p é fatorado. Observe ainda que:

$$5 = (\sqrt{5})^2 = (2\omega - 1)^2 \ ;$$

e isto finaliza a demonstração do teorema. ■

3.2 Decomposição em corpos quadráticos

Nesta seção veremos os tipos de decomposição de primos para os corpos quadráticos, anteriormente apresentadas num contexto mais geral.

Seja $1, \delta$ uma base integral de L, onde $\delta = \sqrt{d}$, $P_{\delta|\mathbb{Q}} = x^2 - d$ no caso em que $d \equiv 2$ ou $3 \bmod 4$, e $\delta = \frac{1+\sqrt{d}}{2}$, $P_{\delta|\mathbb{Q}} = x^2 - x - \frac{d-1}{4}$ no caso em que $d \equiv 1 \bmod 4$. Para todo número primo p, denotamos por k_p o homomorfismo canônico de $\mathbb{Z}[x]$ sobre $\mathbb{F}_p[x]$.

Teorema 3.17 *Seja* $P = P_{\delta|\mathbb{Q}}$. *Para todo número primo* p, *as seguintes condições são equivalentes:*

(i) p *é ramificado em* L.

(ii) *O polinômio $k_pP \in \mathbb{F}_p[x]$ é inseparável.*

(iii) *p é um divisor do discriminante d_L.*

(iv) *p satisfaz uma das seguintes condições:*

a) $p = 2$ e $d \equiv 3 \bmod 4$, ou b) p divide d.

Neste caso temos que $p \cdot I_L = \mathfrak{P}^2$ e $f(\mathfrak{P}) = 1$, onde $\mathfrak{P}$ é o único ideal primo de I_L que está acima de p; além disto,

$$k_pP = (x - k_p1)^2 \text{ e } \mathfrak{P} = (p, \delta - 1) \text{ quando } p = 2 \text{ e } d \equiv 3 \bmod 4;$$
$$k_pP = x^2 \text{ e } \mathfrak{P} = (p, \delta) \text{ quando } p \mid d \text{ e } d \equiv 2 \text{ ou } 3 \bmod 4;$$
$$k_pP = \left(x - k_p\left(\tfrac{d-1}{2}\right)\right)^2 \text{ e } \mathfrak{P} = \left(p, \delta - \tfrac{d-1}{2}\right) \text{ quando } p \mid d \text{ e } d \equiv 1 \bmod 4.$$

Demonstração. A equivalência das condições (i), (ii) e (iii) resulta do corolário A.52. A equivalência entre (iii) e (iv) resulta de que $d_L = 4 \cdot d$ (respectivamente $= d$) no caso em que $d \equiv 2$ ou 3 (respectivamente $\equiv 1$) $\bmod 4$.

Se $d \equiv 3 \bmod 4$, então obviamente

$$k_2P = k_2(x^2 - d) = x^2 - k_2d = (x - k_21)^2.$$

Se p dividir d e $d \equiv 2$ ou $3 \bmod 4$, então $x^2 - k_pd = x^2$. No caso em que $d \equiv 1 \bmod 4$, temos que $P = x^2 - x - t$, sendo $t \in \mathbb{Z}$ tal que $d = 1 + 4t$. Se p dividir d, então:

$$4t \equiv -1 \bmod p \text{ e } 4t^2 \equiv -t \bmod p\ ;$$

logo,

$$k_pP = x^2 + k_p(4t) \cdot x + k_p(4t^2) = (x - k_p(2t))^2 = \left(x - k_p\left(\frac{d-1}{2}\right)\right)^2.$$

O resto resulta do teorema A.50. ■

Teorema 3.18 *Seja $P = P_{\delta|\mathbb{Q}}$. Para todo número primo p, as seguintes condições são equivalentes:*

(i) *p é decomposto em L.*

(ii) *O polinômio $k_pP \in \mathbb{F}_p[x]$ é separável e redutível.*

(iii) *p satisfaz uma das seguintes condições:*

a) $p = 2$ *e* $d \equiv 1 \bmod 8$, *ou*

b) p *é ímpar e* d *é resto quadrático* $\bmod p$.

Neste caso temos que $p \cdot I_L = \mathfrak{P} \cdot \mathfrak{P}'$ *e* $f(\mathfrak{P}) = f(\mathfrak{P}') = 1$, *onde* $\mathfrak{P}$ *e* $\mathfrak{P}'$ *são os únicos ideais primos de* I_L *que estão acima de* p; *além disto,*

$k_pP = x \cdot (x - k_p 1)$ e $\mathfrak{P} = (p, \delta)$, $\mathfrak{P}' = (p, \delta - 1)$ quando $p = 2$, $d \equiv 1 \bmod 8$;

$k_pP = (x - k_p a) \cdot (x + k_p a)$ *e* $\mathfrak{P} = (p, \delta - a)$, $\mathfrak{P}' = (p, \delta + a)$ *quando* p *for ímpar e* $d \equiv 2$ *ou* $3 \bmod 4$, *sendo* $a \in \mathbb{Z}$ *tal que* $d \equiv a^2 \bmod p$;

$k_pP = (x - k_p \mathfrak{g}) \cdot (x - k_p(1 - \mathfrak{g}))$ *e* $\mathfrak{P} = (p, \delta - \mathfrak{g})$, $\mathfrak{P}' = (p, \delta - 1 + \mathfrak{g})$ *quando* p *for ímpar e* $d \equiv 1 \bmod 4$, *sendo* $\mathfrak{g} \in \mathbb{Z}$ *tal que* $d \equiv (2\mathfrak{g} + 1)^2 \bmod p$.

Demonstração. (i) $\iff$ (ii) resulta do teorema A.50.

(ii) $\implies$ (iii): Existem $a, b \in \mathbb{Z}$ tais que:

$$k_pP = (x - k_p a) \cdot (x - k_p b) \text{ e } a \equiv b \bmod p.$$

Pelo teorema 3.17, resulta que p não divide d e que $d \equiv 2$ *ou* $3 \bmod 4$ implica $p \neq 2$. No caso em que $d \equiv 2$ *ou* $3 \bmod 4$, temos que:

$$a + b \equiv 0 \mod p \text{ e } a^2 \equiv -a \cdot b \equiv d \mod p \ ;$$

logo d é um resto quadrático $\bmod p$. No caso em que $d \equiv 1 \bmod 4$, temos que $a + b \equiv 1 \bmod p$ e

$$a^2 - a \equiv -a \cdot b \equiv \frac{d-1}{4} \bmod p.$$

Para $p = 2$, temos:

$$a^2 \equiv a \mod 2 \implies \frac{d-1}{4} \equiv 0 \mod 2 \implies d \equiv 1 \mod 8.$$

Se $p \neq 2$, então:

$$(2a - 1)^2 = 4 \cdot (a^2 - a) + 1 \equiv d \mod p \ ,$$

logo d é um resto quadrático $\bmod p$.

(iii) $\implies$ (ii): Suponhamos que $p = 2$ e $d \equiv 1 \bmod 8$. Então,

$$\frac{d-1}{4} \equiv 0 \mod 2 \implies k_2P = x \cdot (x - k_2 1).$$

Suponhamos que p seja ímpar e $d \equiv a^2 \bmod p$ para algum $a \in \mathbb{Z}$. No caso em que $d \equiv 2$ *ou* $3 \bmod 4$, temos que:

$$k_pP = (x - k_p a) \cdot (x + k_p a), \text{ e } k_p a \neq -k_p a \text{ pois } 2a \equiv 0 \mod p.$$

No caso em que $d \equiv 1 \bmod 4$, temos que $P = x^2 - x - t$, sendo $t \in \mathbb{Z}$ tal que $d = 1 + 4t$. Seja $\mathfrak{g} \in \mathbb{Z}$ tal que $2\mathfrak{g} \equiv a + 1 \bmod p$; então:

$$d \equiv a^2 \equiv (2\mathfrak{g} - 1)^2 \bmod p \implies 4t \equiv a^2 - 1 \equiv 4\mathfrak{g} \cdot (\mathfrak{g} - 1) \bmod p,$$

e assim,

$$-k \equiv \mathfrak{g} \cdot (1 - \mathfrak{g}) \bmod p \text{ e } k_p P = (x - k_p\mathfrak{g}) \cdot (x - k_p(1 - \mathfrak{g})).$$

Além disto, temos que $k_p\mathfrak{g} \neq k_p(1 - \mathfrak{g})$, pois $2 \cdot \mathfrak{g} - 1 \equiv a \equiv 0 \bmod p$. Em todos os casos, $k_p P$ é separável e redutível em $\mathbb{F}_p[x]$. O resto resulta do teorema A.50. ■

Do fato de que os números primos inertes em L são exatamente os que não são nem ramificados nem decompostos em L resulta imediatamente o seguinte:

Corolário 3.19 *Seja $P = P_{\delta|\mathbb{Q}}$. Para todo número primo p, as seguintes condições são equivalentes:*

(i) *p é inerte em L.*

(ii) *O polinômio $k_p P$ é irredutível em $\mathbb{F}_p[x]$.*

(iii) *p satisfaz uma das seguintes condições:*

a) $p = 2$ e $d \equiv 5 \bmod 8$, ou

b) p é ímpar e d é não-resto quadrático $\bmod p$.

Neste caso, $p \cdot I_L$ é um ideal primo de I_L e $f(p \cdot I_L) = 2$. ■

3.3 Soma de dois quadrados em $\mathbb{Q}(\sqrt{5})$

Nesta seção veremos que todo inteiro algébrico totalmente positivo de $\mathbb{Q}(\sqrt{5})$ tem uma representação em soma de dois quadrados de inteiros de $I_{\mathbb{Q}(\sqrt{5})}$. Este resultado será muito importante na demonstração do nosso principal resultado, que será visto logo em seguida.

Seja $I_{\mathbb{Q}(\sqrt{5})}$ denotar o anel dos inteiros algébricos de $\mathbb{Q}(\sqrt{5})$. Como $5 \equiv 1 \bmod 4$, temos pelo teorema 3.6 que:

$$I_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[1, \varepsilon], \text{ onde } \varepsilon = \frac{1 + \sqrt{5}}{2}.$$

Definição 3.20 *Seja $\alpha = a + b \cdot \sqrt{5} \in \mathbb{Q}(\sqrt{5})$. O número $\overline{\alpha} = a - b \cdot \sqrt{5}$ é denominado o* conjugado *do número α no corpo $\mathbb{Q}(\sqrt{5})$.*

Lema 3.21 *Seja $k \in I_{\mathbb{Q}(\sqrt{5})}$. Então, existe $x \in \mathbb{Z}$ tal que $k \cdot \overline{k} \equiv -x^2 \bmod 5$.*

Demonstração. Seja $k = a + b \cdot \varepsilon$, onde $a, b \in \mathbb{Z}$. Então:

$$\begin{aligned} k \cdot \overline{k} &= (a + b \cdot \varepsilon) \cdot (a + b \cdot \overline{\varepsilon}) = a^2 + ab\overline{\varepsilon} + ab\varepsilon + b^2\varepsilon\overline{\varepsilon} \\ &= a^2 + ab\left(\frac{1-\sqrt{5}}{2} + \frac{1+\sqrt{5}}{2}\right) + \frac{b^2}{4}(1-5) \\ &= a^2 + ab - b^2; \end{aligned}$$

ou seja,

$$k \cdot \overline{k} + b^2 = a^2 + ab \implies k \cdot \overline{k} + b^2 \equiv (a^2 + ab) \bmod 5. \tag{3.7}$$

Por outro lado, temos:

$$a^2 + ab \equiv (-4a^2 - 4ab) \bmod 5. \tag{3.8}$$

De (3.7) e (3.8), segue que:

$$k \cdot \overline{k} + b^2 \equiv (-4a^2 - 4ab) \bmod 5 \implies k \cdot \overline{k} \equiv (-4a^2 - 4ab - b^2) \bmod 5;$$

portanto, $k \cdot \overline{k} \equiv -(2a + b)^2 \bmod 5$ e fazendo $x = 2a + b$ o resultado segue. ■

Lema 3.22 (Artifício de Euler) *Sejam $\alpha, \beta \in \mathbb{R}$. Então:*

$$\left(\frac{\alpha+\beta}{2}\right)^2 + \left(\frac{\alpha-\beta}{2}\right)^2 = \frac{\alpha^2+\beta^2}{2}.$$

Demonstração. Observe que:

$$\left(\frac{\alpha+\beta}{2}\right)^2 + \left(\frac{\alpha-\beta}{2}\right)^2 = \frac{2\alpha^2+2\beta^2}{4} = \frac{\alpha^2+\beta^2}{2};$$

e, portanto o resultado segue. ■

Lema 3.23 *Se -1 é um quadrado $\bmod p$, então -5 também o é, no anel dos inteiros $I_{\mathbb{Q}(\sqrt{5})}$. Além disso, existem $x, y \in I_{\mathbb{Q}(\sqrt{5})}$ tais que $x^2 + 5y^2 \equiv 0 \bmod p$.*

Demonstração. Como -1 é um quadrado $\bmod p$, existe $y \in I_{\mathbb{Q}(\sqrt{5})}$ tal que:

$$y^2 \equiv -1 \bmod p \implies 5y^2 \equiv -5 \bmod p \implies (\sqrt{5}y)^2 \equiv -5 \bmod p.$$

Fazendo $z = \sqrt{5}y$, temos que:

$$z^2 \equiv -5 \bmod p\ ,$$

ou seja, -5 é um quadrado $\bmod p$.

Observe ainda que:

$$y^2 \cdot z^2 \equiv 5 \bmod p \implies (y \cdot z)^2 \equiv 5 \bmod p.$$

Faça $x = y \cdot z$ e então $x^2 \equiv 5 \bmod p$. Como $-1 \equiv y^2 \bmod p$, temos:

$$-x^2 \equiv 5y^2 \bmod p \ ;$$

ou seja, $x^2 + 5y^2 \equiv 0 \bmod p$. ■

Lema 3.24 *Seja $p \in \mathbb{Z}$ um número primo tal que $p \equiv -1 \bmod 4$ e, $\nu \in I_{\mathbb{Q}(\sqrt{5})}$ satisfazendo $\nu^2 \equiv -5 \bmod p$. Então, ν pode ser escolhido como um racinal inteiro em $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(p)}$.*

Demonstração. Desde que $\nu^2 \equiv -5 \bmod p$, temos:

$$\overline{\nu}^2 \equiv -5 \bmod p \implies \nu^2 \equiv \overline{\nu}^2 \bmod p \implies (\nu + \overline{\nu}) \cdot (\nu - \overline{\nu}) \equiv 0 \bmod p.$$

Como p é primo temos que:

$$\nu + \overline{\nu} \equiv 0 \bmod p \ \text{ ou } \ \nu - \overline{\nu} \equiv 0 \bmod p.$$

Se $\nu + \overline{\nu} \equiv 0 \bmod p$, então escrevendo $\nu = a + b \cdot \varepsilon$ com $a, b \in \mathbb{Z}$, temos:

$$a + b \cdot \varepsilon + a + b \cdot \overline{\varepsilon} \equiv 0 \bmod p \implies 2a + b \equiv 0 \bmod p.$$

Observe ainda que:

$$\nu - \frac{b\sqrt{5}}{2} = a + \frac{b + b\sqrt{5}}{2} - \frac{b\sqrt{5}}{2} = a + \frac{b}{2} = \frac{2a + b}{2};$$

portanto,

$$\nu \equiv \frac{b\sqrt{5}}{2} \bmod p \implies \nu^2 \equiv \frac{5b^2}{4} \bmod p.$$

Como $\nu^2 \equiv -5 \bmod p$, então:

$$-5 \equiv \frac{5b^2}{4} \bmod p \implies 5 \cdot (-4 - b^2) \in (p).$$

Como $I_{\mathbb{Q}(\sqrt{5})}$ é um domínio de Dedekind, então (p) é maximal e $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(p)}$ é um corpo. Tomando o inverso multiplicativo do 5 neste corpo, concluímos que:

$$-4 \equiv b^2 \bmod p.$$

Como $b \equiv -2a \bmod p$, então:

$$b^2 \equiv 4a^2 \bmod p \implies -4 \equiv 4a^2 \bmod p \implies -1 \equiv a^2 \bmod p.$$

Portanto, -1 é resto quadrático em $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Isto é uma contradição, uma vez que $p \equiv -1 \bmod 4$.

Podemos concluir que $\nu - \overline{\nu} \equiv 0 \bmod p$, ou seja:

$$a + b \cdot \varepsilon - a - b \cdot \overline{\varepsilon} \equiv 0 \bmod p \implies b\sqrt{5} \equiv 0 \bmod p \implies 5b^2 \equiv 0 \bmod p,$$

ou seja:

$$b^2 \equiv 0 \bmod p \implies b \equiv 0 \bmod p,$$

pois p é primo. Então, $\nu = a + b \cdot \varepsilon \equiv a \bmod p$, com $a \in \mathbb{Z}$. ■

Teorema 3.25 *Um primo ρ de $I_{\mathbb{Q}(\sqrt{5})}$ para o qual -1 é um resto quadrático tem uma representação $k \cdot \rho = x^2 + y^2$, onde $x, y \in I_{\mathbb{Q}(\sqrt{5})}$ e k é uma unidade.*

Demonstração. Seja o primo ρ estar acima do primo p de $\mathbb{Z}$. Pela observação A.49, existem três possibilidades, a saber, p pode se ramificar, p pode se decompor ou p pode ser inerte.

Se p ramifica então, pelo teorema 3.17 temos que:

$$p = 5 \text{ e } 5 \cdot I_{\mathbb{Q}(\sqrt{5})} = \mathfrak{P}^2 \text{ com } f(\mathfrak{P}) = 1,$$

onde $\mathfrak{P}$ é o único ideal primo de $I_{\mathbb{Q}(\sqrt{5})}$ acima de 5. Portanto, utilizando a proposição A.26 e o teorema A.29, temos:

$$\rho \cdot I_{\mathbb{Q}(\sqrt{5})} = \mathfrak{P} \implies \mathfrak{N}\left(\rho \cdot I_{\mathbb{Q}(\sqrt{5})}\right) = \mathfrak{N}(\mathfrak{P}) = 5^{f(\mathfrak{P})} = 5^1 = 5 = |\mathcal{N}(\rho)|,$$

ou seja, $\mathcal{N}(\rho) = \pm 5$. Pelo teorema 3.16, temos que $\rho = \varepsilon^t \cdot \sqrt{5}$, onde ε é uma unidade. Mas,

$$\varepsilon \cdot \sqrt{5} = \left(\frac{1+\sqrt{5}}{2}\right) \cdot \sqrt{5} = \frac{\sqrt{5}+5}{2} = \frac{3+\sqrt{5}}{2} + 1. \tag{3.9}$$

Observe ainda que:

$$\varepsilon^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2}. \tag{3.10}$$

De (3.9) e (3.10), temos que $\varepsilon \cdot \sqrt{5} = \varepsilon^2 + 1$. Portanto:

$$\rho = \varepsilon^t \cdot \sqrt{5} = \varepsilon^{t-1} \cdot \varepsilon\sqrt{5} = \varepsilon^{t-1} \cdot (\varepsilon^2 + 1) \implies \varepsilon^{1-t} \cdot \rho = \varepsilon^2 + 1^2.$$

Tomando $k = \varepsilon^{1-t}$, temos:

$$k \cdot \rho = \varepsilon^2 + 1^2, \text{ com } k \in U\left(I_{\mathbb{Q}(\sqrt{5})}\right).$$

Se p se decompõe, temos pelo teorema 3.18, que:

$$p \cdot I_{\mathbb{Q}(\sqrt{5})} = \mathfrak{P} \cdot \mathfrak{P}' \quad \text{e} \quad f(\mathfrak{P}) = f(\mathfrak{P}') = 1,$$

onde $\mathfrak{P}$ e $\mathfrak{P}'$ são os únicos ideais primos de $I_{\mathbb{Q}(\sqrt{5})}$ que estão acima de p. Portanto, $\rho \cdot I_{\mathbb{Q}(\sqrt{5})} = \mathfrak{P}$ ou $\rho \cdot I_{\mathbb{Q}(\sqrt{5})} = \mathfrak{P}'$. Utilizando a proposição A.26 e o teorema A.29, temos:

$$\mathfrak{N}\left(\rho \cdot I_{\mathbb{Q}(\sqrt{5})}\right) = \mathfrak{N}(\mathfrak{P}) = \mathfrak{N}(\mathfrak{P}') = p^f = p = |\mathcal{N}(\rho)| = |\rho \cdot \overline{\rho}|. \tag{3.11}$$

Seja $\lambda \in I_{\mathbb{Q}(\sqrt{5})}$ tal que $\lambda^2 \equiv -1 \bmod \rho$ e considere o seguinte conjunto:

$$M = \mathbb{Z} \cdot (1, 1, \lambda, \overline{\lambda}) + \mathbb{Z} \cdot (\varepsilon, \overline{\varepsilon}, \lambda\varepsilon, \overline{\lambda\varepsilon}) + \mathbb{Z} \cdot (0, 0, \rho, \overline{\rho}) + \mathbb{Z} \cdot (0, 0, \varepsilon\rho, \overline{\varepsilon\rho}).$$

Pelo lema 2.11, definição 2.16 e pela equação (3.11), temos que:

$$\begin{aligned} Vol(M) &= Vol(T_v) = \left|\det \begin{pmatrix} 1 & 1 & \lambda & \overline{\lambda} \\ \varepsilon & \overline{\varepsilon} & \lambda\varepsilon & \overline{\lambda\varepsilon} \\ 0 & 0 & \rho & \overline{\rho} \\ 0 & 0 & \varepsilon\rho & \overline{\varepsilon\rho} \end{pmatrix}\right| = \left|\det \begin{pmatrix} 1 & 1 & \lambda & \overline{\lambda} \\ 0 & \overline{\varepsilon} - \varepsilon & 0 & \overline{\lambda} \cdot (\overline{\varepsilon} - \varepsilon) \\ 0 & 0 & \rho & \overline{\rho} \\ 0 & 0 & 0 & \overline{\rho} \cdot (\overline{\varepsilon} - \varepsilon) \end{pmatrix}\right| \\ &= \left|(\overline{\varepsilon} - \varepsilon)^2 \cdot \rho \cdot \overline{\rho}\right| = 5 \cdot |\rho \cdot \overline{\rho}| = 5 \cdot p \neq 0. \end{aligned}$$

Pelo lema 2.12, M é um reticulado em $\mathbb{R}^4$ com base $\{(1, 1, \lambda, \overline{\lambda}), (\varepsilon, \overline{\varepsilon}, \lambda\varepsilon, \overline{\lambda\varepsilon}), (0, 0, \rho, \overline{\rho}), (0, 0, \varepsilon\rho, \overline{\varepsilon\rho})\}$. Observe que um ponto qualquer deste reticulado tem a forma:

$$x \cdot (1, 1, \lambda, \overline{\lambda}) + y \cdot (\varepsilon, \overline{\varepsilon}, \lambda\varepsilon, \overline{\lambda\varepsilon}) + z \cdot (0, 0, \rho, \overline{\rho}) + w \cdot (0, 0, \varepsilon\rho, \overline{\varepsilon\rho}) \ (x, y, z, w \in \mathbb{Z}) \ ;$$

ou seja,

$$(x + y\varepsilon, x + y\overline{\varepsilon}, (x + y\varepsilon) \cdot \lambda + (z + w\varepsilon) \cdot \rho, (x + y\overline{\varepsilon}) \cdot \overline{\lambda} + (z + w\overline{\varepsilon}) \cdot \overline{\rho}).$$

Fazendo:

$$\begin{cases} \alpha = x + y\varepsilon \\ \mu = z + w\varepsilon \end{cases} \Longrightarrow \begin{cases} \overline{\alpha} = x + y\overline{\varepsilon} \\ \overline{\mu} = z + w\overline{\varepsilon} \end{cases} ;$$

onde α, μ percorrem todo o anel $I_{\mathbb{Q}(\sqrt{5})}$. Daí, os elementos típicos do reticulado são dados por:

$$(\alpha, \overline{\alpha}, \alpha \cdot \lambda + \mu \cdot \rho, \overline{\alpha} \cdot \overline{\lambda} + \overline{\mu} \cdot \overline{\rho}). \tag{3.12}$$

Seja $B_4(r)$ a bola de raio r centrada na origem, em $\mathbb{R}^4$, tal que $r^2 = (4,1)\cdot\sqrt{p}$. Pelo lema 2.31, temos:

$$Vol(B_4(r)) = \frac{\pi^2}{2}\cdot r^4 = \frac{\pi^2}{2}\cdot(4,1)^2\cdot p \cong (82,87)\cdot p > 80\cdot p = 2^4\cdot 5p = 2^4\cdot Vol(M).$$

Então, pelo corolário 2.23, existe um ponto não-nulo do reticulado no interior de $B_4(r)$. Em virtude de (3.12), tal ponto tem a forma:

$$(\alpha,\overline{\alpha},\beta,\overline{\beta}),\ \text{ com }\ \alpha,\beta\in I_{_{\mathbb{Q}(\sqrt{5})}}.$$

Além disso,

$$\alpha^2+\beta^2 = \alpha^2+(\lambda\alpha+\mu\rho)^2 = \underbrace{\alpha^2\cdot(1+\lambda^2)}_{\equiv 0 \bmod\rho} + \underbrace{(2\lambda\alpha\mu+\mu^2\rho)\cdot\rho}_{\equiv 0 \bmod\rho};$$

então, $\alpha^2+\beta^2\equiv 0 \bmod\rho$ e nós podemos escrever:

$$\alpha^2+\beta^2 = k\cdot\rho,\ \text{ com }\ k\in I_{_{\mathbb{Q}(\sqrt{5})}}. \tag{3.13}$$

Daí,

$$\left\|(\alpha,\overline{\alpha},\beta,\overline{\beta})\right\| < r \implies \alpha^2+\overline{\alpha}^2+\beta^2+\overline{\beta}^2 < (4,1)\cdot\sqrt{p};$$

e de (3.13), segue que:

$$k\rho+\overline{k\rho} < (4,1)\cdot\sqrt{p}. \tag{3.14}$$

Observe ainda que:

$$(k\rho-\overline{k\rho})^2\geq 0 \implies (k\rho)^2+(\overline{k\rho})^2\geq 2\cdot k\rho\cdot\overline{k\rho}. \tag{3.15}$$

Por outro lado, utilizando (3.15), temos:

$$(k\rho+\overline{k\rho})^2 = (k\rho)^2+(\overline{k\rho})^2+2\cdot k\rho\cdot\overline{k\rho}\geq 2\cdot k\rho\cdot\overline{k\rho}+2\cdot k\rho\cdot\overline{k\rho};$$

como $k\rho$ é totalmente positivo, obtemos:

$$(k\rho+\overline{k\rho})^2\geq 4\cdot k\rho\cdot\overline{k\rho} \implies k\rho+\overline{k\rho}\geq 2\cdot\sqrt{k\rho\cdot\overline{k\rho}}. \tag{3.16}$$

De (3.14) e (3.16), segue que:

$$2\cdot\sqrt{k\rho\cdot\overline{k\rho}}\leq k\rho+\overline{k\rho} < (4,1)\cdot\sqrt{p} \implies \sqrt{k\rho\cdot\overline{k\rho}} < (2,05)\cdot\sqrt{p};$$

ou seja,

$$k\rho\cdot\overline{k\rho} < (4,2025)\cdot p \implies \left|k\overline{k}\rho\overline{\rho}\right| < (4,2025)\cdot p \implies \left|k\overline{k}\right|\cdot|\rho\overline{\rho}| < (4,2025)\cdot p.$$

De (3.9), concluimos que:

$$\left|k\overline{k}\right| \cdot p < (4,2025) \cdot p \implies \left|k\overline{k}\right| \leq 4.$$

Pelo lema 3.21, temos que $k\overline{k}$ é o negativo de um quadrado $\bmod 5$ e estes são apenas 0 e ± 1. Como $\mathcal{N}(k) = k\overline{k}$ e $\mathcal{N}(k\overline{k}) = \mathcal{N}(k) \cdot \mathcal{N}(\overline{k})$, segue que $\mathcal{N}(k), \mathcal{N}(k\overline{k}) \neq \pm 2, \pm 3$. Certamente, $\mathcal{N}(k) \neq 0$.

Se $\mathcal{N}(k) = \pm 1$, então k é uma unidade e nós finalizamos. Caso contrário, temos que:

$$\mathcal{N}(k) = \mathcal{N}(\overline{k}) = \pm 4.$$

Desde que $d = 5 \equiv 5 \bmod 8$, temos pelo corolário 3.19 que 2 é inerte em $\mathbb{Q}(\sqrt{5})$, ou seja, 2 permanece primo em $I_{\mathbb{Q}(\sqrt{5})}$ e $\mathcal{N}(2) = 4$. Como,

$$2 \mid \pm 4 = \mathcal{N}(k) = k\overline{k} \implies 2 \mid k \text{ ou } 2 \mid \overline{k} \implies 2 \mid k, \overline{k}.$$

Escrevendo $k = 2\mu$, temos:

$$\mathcal{N}(k) = \mathcal{N}(2\mu) = \mathcal{N}(2) \cdot \mathcal{N}(\mu) \implies \pm 4 = 4 \cdot \mathcal{N}(\mu) \implies \mathcal{N}(\mu) = \pm 1;$$

ou seja, μ é uma unidade.

Portanto, temos de (3.13) que:

$$\alpha^2 + \beta^2 = k \cdot \rho = 2 \cdot \mu \cdot \rho.$$

Note ainda que:

$$\alpha^2 + \beta^2 \equiv 0 \bmod(2) \implies (\alpha + \beta)^2 = \alpha^2 + \beta^2 + 2\alpha\beta \equiv 0 \bmod(2).$$

Como 2 é primo em $I_{\mathbb{Q}(\sqrt{5})}$ temos que $2 \mid (\alpha + \beta)$. De forma análoga, temos que $2 \mid (\alpha - \beta)$. Daí, $\frac{\alpha \pm \beta}{2} \in I_{\mathbb{Q}(\sqrt{5})}$. Para finalizar, nós utilizamos o lema 3.22 e obtemos:

$$\left(\frac{\alpha + \beta}{2}\right)^2 + \left(\frac{\alpha - \beta}{2}\right)^2 = \frac{\alpha^2 + \beta^2}{2} = \frac{2 \cdot \mu \cdot \rho}{2} = \mu \cdot \rho \ ,$$

isto dá a necessária representação.

Se p permanece inerte em $I_{\mathbb{Q}(\sqrt{5})}$, existem dois casos além do caso trivial de 2.

1º) Quando $p \equiv 1 \bmod 4$, temos pelo lema 2.28 que -1 é resto quadrático $\bmod p$ e o teorema segue facilmente do teorema 2.29.

2^o) Quando $p \equiv -1 \bmod 4$, então existem algumas vezes em que p é a soma de dois quadrados em $I_{\mathbb{Q}(\sqrt{5})}$, por exemplo:

$$\begin{aligned} \varepsilon^2 + \overline{\varepsilon}^2 &= \left(\frac{1+\sqrt{5}}{2}\right)^2 + \left(\frac{1-\sqrt{5}}{2}\right)^2 \\ &= \frac{1+2\sqrt{5}+5+1-2\sqrt{5}+5}{4} = \frac{12}{4} = 3. \end{aligned}$$

Como p é primo e $I_{\mathbb{Q}(\sqrt{5})}$ é um domínio de Dedekind, então $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(p)}$ é um corpo. Observe ainda que:

$$\begin{aligned} \frac{I_{\mathbb{Q}(\sqrt{5})}}{(p)} &= \left\{x + p \cdot I_{\mathbb{Q}(\sqrt{5})} : x \in I_{\mathbb{Q}(\sqrt{5})}\right\} \\ &= \{a + b\varepsilon + p \cdot (c + d\varepsilon) : a, b, c, d \in \mathbb{Z}\} \\ &= \{a + pc + (b + pd)\varepsilon : a, b, c, d \in \mathbb{Z}\} \\ &= \{\overline{a} + \overline{b}\varepsilon : \overline{a}, \overline{b} \in \mathbb{Z}_p\}. \end{aligned}$$

Daí, $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(p)}$ é um corpo com p^2 elementos. Também é razoável que uma raiz quadrada de -1 aparecerá em certos casos. Portanto, em virtude do lema 3.23, faz sentido considerar o problema de representação deste p pela forma quadrática x^2+5y^2 sobre os racionais inteiros.

Seja $\nu \in I_{\mathbb{Q}(\sqrt{5})}$ tal que $\nu^2 \equiv -5 \bmod p$. Em virtude do lema 3.24, temos:

$$\nu \equiv a \mod p \text{ com } a \in \mathbb{Z}.$$

Seja l o inverso multiplicativo de ν com respeito ao corpo $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(p)}$. Temos que $l = c+d\varepsilon$, onde $c, d \in \mathbb{Z}$. Observe que:

$$\nu \cdot l - 1 \in p \cdot I_{\mathbb{Q}(\sqrt{5})} \implies a \cdot (c + d\varepsilon) - 1 = p \cdot (s + t\varepsilon) \implies ac - ps - 1 + (ad - pt)\varepsilon = 0 \ ;$$

portanto,

$$\begin{cases} ac - ps - 1 = 0 \implies \overline{a} \cdot \overline{c} = 1 \implies \overline{c} = (\overline{a})^{-1} = (\overline{\nu})^{-1} = \overline{l} \\ ad - pt = 0 \implies \overline{a} \cdot \overline{d} = \overline{0} \implies \overline{d} = \overline{0}, \text{ pois } \overline{a} \neq \overline{0}. \end{cases}$$

Portanto, l pode ser escolhido como um racional inteiro módulo p.

Considere o subconjunto do $\mathbb{R}^2$ dado por $M = \mathbb{Z} \cdot (1; l) + \mathbb{Z} \cdot (0; p)$. Pelo lema 2.11 e a definição 2.16, temos:

$$Vol(M) = \left|\det \begin{pmatrix} 1 & l \\ 0 & p \end{pmatrix}\right| = p \neq 0.$$

Pelo lema 2.12, M é um reticulado com base $\{(1;l),(0;p)\}$. Considere a elipse da forma $x^2+5y^2=r^2$, centrada na origem, ou seja:

$$\frac{x^2}{r^2}+\frac{y^2}{\frac{r^2}{5}}=1 \implies a=r \text{ e } b=\frac{r\sqrt{5}}{5},$$

onde a,b são os semi-eixos da mesma. Do cálculo, sabemos que a área dessa elipse é dada por:

$$\pi\cdot a\cdot b=\pi\cdot r\cdot\frac{r\sqrt{5}}{5}=\pi\cdot\frac{r^2\sqrt{5}}{5}.$$

Para aplicarmos o teorema de Minkowski (corolário 2.23) para a elipse, devemos ter:

$$\pi\cdot\frac{r^2\sqrt{5}}{5}>2^2\cdot Vol(M)=4p \implies r^2>\frac{4\sqrt{5}}{\pi}\cdot p \implies r^2>(2,85)\cdot p.$$

Fixe $r^2=(2,9)\cdot p$. Um ponto não nulo do reticulado no interior da elipse é da forma:

$$m\cdot(1;l)+n\cdot(0;p)=(m\ ;\ m\cdot l+n\cdot p),\ \text{ com }\ m,n\in\mathbb{Z}.$$

Então, $x=m$ e $y=m\cdot l+n\cdot p$ são tais que:

$$x^2+5y^2=m^2+5\cdot(m\cdot l+n\cdot p)^2=m^2+5m^2l^2+10lmnp+5n^2p^2;$$

daí, segue que:

$$x^2+5y^2\equiv m^2(1+5l^2)\bmod p \implies \overline{x^2+5y^2}=\overline{m^2}\cdot\left(\overline{1+5l^2}\right);$$

mas,

$$\overline{1+5l^2}=\overline{1}+\overline{5}\cdot\overline{l}^2=\overline{1}+\overline{5}\cdot(\overline{\nu}^2)^{-1}=\overline{1}+\overline{5}\cdot(\overline{-5})^{-1}=\overline{1}-\overline{1}=\overline{0}.$$

Portanto,

$$x^2+5y^2\equiv m^2(1+5l^2)\equiv 0\bmod p \tag{3.17}$$

Mas,

$$0<x^2+5y^2<(2,9)\cdot p<3p \tag{3.18}$$

De (3.17) e (3.18), temos que:

$$x^2+5y^2=p \text{ ou } x^2+5y^2=2p.$$

Se $p=x^2+5y^2$, então:

$$p=x^2+(\sqrt{5}y)^2.$$

Para $2p = x^2 + 5y^2$, temos:

$$2p = x^2 + y^2 + 4y^2 = x^2 + 2xy + y^2 - 2xy + 4y^2;$$

portanto,

$$0 \equiv (x+y)^2 \bmod 2 \implies x + y \equiv 0 \bmod 2.$$

Fazendo $b = -y$, temos que $x = b + 2a$ para $a, b \in \mathbb{Z}$. Então:

$$\begin{aligned}
(a+b\varepsilon)^2 + (a+b\overline{\varepsilon})^2 &= 2a^2 + 2ab(\varepsilon + \overline{\varepsilon}) + b^2(\varepsilon^2 + \overline{\varepsilon}^2) \\
&= 2a^2 + 2ab + b^2 \cdot \left(\frac{1 + 2\sqrt{5} + 5 + 1 - 2\sqrt{5} + 5}{4} \right) \\
&= 2a^2 + 2ab + 3b^2 = \frac{1}{2}(4a^2 + 4ab + 6b^2) \\
&= \frac{1}{2}(4a^2 + 4ab + b^2 + 5b^2) = \frac{1}{2}((2a+b)^2 + 5b^2) \\
&= \frac{1}{2}(x^2 + 5y^2) = \frac{1}{2} \cdot 2p \\
&= p
\end{aligned}$$

Em todos os casos, o primo (vezes uma apropriada unidade se necessário) é a soma de dois quadrados do anel dos inteiros algébricos $I_{\mathbb{Q}(\sqrt{5})}$. ■

3.4 Soma de quatro quadrados em $\mathbb{Q}(\sqrt{5})$

Nesta seção provaremos o teorema de Götzky de soma de quatro quadrados, que é o objetivo do nosso trabalho. Para tanto, utilizaremos um reticulado em $\mathbb{R}^8$ e uma nova região convexa, uma vez que a esfera do $\mathbb{R}^8$ não dá um limitante suficientemente bom para aplicar o critério de Minkowski.

Lema 3.26 *Seja $B_4(r_1)$ a bola fechada de raio r_1 centrada na origem em $\mathbb{R}^4$. Seja $r = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}$ a distância de um ponto do $\mathbb{R}^4$ à origem. Seja g uma função contínua de uma variável e $G(x_1, x_2, x_3, x_4) = g(r)$. Então:*

$$\int_{B_4(r_1)} G = 2\pi^2 \cdot \int_{r=0}^{r_1} g(r) r^3 dr.$$

Demonstração. Usando coordenadas esféricas, temos:

$$\begin{cases}
x_1 = r\cos(\theta_1) \\
x_2 = r\sin(\theta_1)\cos(\theta_2) \\
x_3 = r\sin(\theta_1)\sin(\theta_2)\cos(\theta_3) \\
x_4 = r\sin(\theta_1)\sin(\theta_2)\sin(\theta_3)
\end{cases}, \text{ com } 0 < \theta_1, \theta_2 < \pi,\ 0 < \theta_3 < 2\pi \text{ e } r > 0.$$

Utilizando o teorema de Jacobi, temos que o jacobiano desta transformação é dado por:

$$J = \begin{vmatrix} \frac{\partial G^1}{\partial r} & \frac{\partial G^1}{\partial \theta_1} & \frac{\partial G^1}{\partial \theta_2} & \frac{\partial G^1}{\partial \theta_3} \\ \frac{\partial G^2}{\partial r} & \frac{\partial G^2}{\partial \theta_1} & \frac{\partial G^2}{\partial \theta_2} & \frac{\partial G^2}{\partial \theta_3} \\ \frac{\partial G^3}{\partial r} & \frac{\partial G^3}{\partial \theta_1} & \frac{\partial G^3}{\partial \theta_2} & \frac{\partial G^3}{\partial \theta_3} \\ \frac{\partial G^4}{\partial r} & \frac{\partial G^4}{\partial \theta_1} & \frac{\partial G^4}{\partial \theta_2} & \frac{\partial G^4}{\partial \theta_3} \end{vmatrix} = r^3 \sin^2(\theta_1)\sin(\theta_2).$$

Daí, segue que:

$$\begin{aligned} \int_{B_4(r_1)} G &= \int_{r=0}^{r_1}\int_{\theta_1=0}^{\pi}\int_{\theta_2=0}^{\pi} g(r)r^3\sin^2(\theta_1)\sin(\theta_2)\ dr\ d\theta_1\ d\theta_2 \left[\theta_3 \Big|_0^{2\pi}\right] \\ &= 2\pi\cdot\int_{r=0}^{r_1}\int_{\theta_1=0}^{\pi} g(r)r^3\sin^2(\theta_1)\ dr\ d\theta_1 \left[-\cos(\theta_2)\Big|_0^{\pi}\right] \\ &= 2\pi\cdot 2\cdot\int_{r=0}^{r_1} g(r)r^3\ dr\left[\ \frac{\theta_1}{2}\Big|_0^{\pi} - \frac{1}{4}\sin(2\theta_1)\Big|_0^{\pi}\right] \\ &= 2\pi\cdot 2\cdot\frac{\pi}{2}\cdot\int_{r=0}^{r_1} g(r)r^3\ dr\ ; \end{aligned}$$

portanto, $\int_{B_4(r_1)} G = 2\pi^2\cdot\int_{r=0}^{r_1} g(r)r^3dr$. ■

Veremos a seguir um resultado básico da análise, que será útil para o estudo da convexidade da nossa nova região.

Lema 3.27 *Seja S um subconjunto do $\mathbb{R}^n$. S é convexa se, e somente se, o ponto médio do segmento que une quaisquer dois pontos de S, pertence a S.* ■

Lema 3.28 *A região $\mathcal{C} = \mathcal{C}(r)$ em $\mathbb{R}^8$, definida por:*

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

é uma região convexa centralmente simétrica com volume $\frac{\pi^4}{280}r^8$.

Demonstração. É óbvio que $\mathcal{C}$ é centralmente simétrica. Antes de mostrarmos a convexidade, lembramos que se $w = (w_1, w_2, w_3, w_4), z = (z_1, z_2, z_3, z_4) \in \mathbb{R}^4$, temos pela desigualdade triangular que $\|w+z\| \leq \|w\| + \|z\|$, ou seja:

$$\sqrt{(w_1+z_1)^2+\cdots+(w_4+z_4)^2} \leq \sqrt{w_1^2+\cdots+w_4^2} + \sqrt{z_1^2+\cdots+z_4^2}. \tag{3.19}$$

Dados dois pontos em $\mathcal{C}$, em virtude do lema 3.23, precisamos apenas mostrar que o ponto médio do segmento que une estes dois pontos está também em $\mathcal{C}$. Mas, se

$(x_1,\ldots,x_8),(y_1,\ldots,y_8)\in\mathcal{C}$ temos, por (3.19) que:

$$\begin{aligned}
&\sqrt{\left(\frac{x_1+y_1}{2}\right)^2+\cdots+\left(\frac{x_4+y_4}{2}\right)^2}+\sqrt{\left(\frac{x_5+y_5}{2}\right)^2+\cdots+\left(\frac{x_8+y_8}{2}\right)^2}\\
&\quad\leq\sqrt{\left(\frac{x_1}{2}\right)^2+\cdots+\left(\frac{x_4}{2}\right)^2}+\sqrt{\left(\frac{y_1}{2}\right)^2+\cdots+\left(\frac{y_4}{2}\right)^2}\\
&\quad+\sqrt{\left(\frac{x_5}{2}\right)^2+\cdots+\left(\frac{x_8}{2}\right)^2}+\sqrt{\left(\frac{y_5}{2}\right)^2+\cdots+\left(\frac{y_8}{2}\right)^2}\\
\leq\;&\frac{1}{2}\sqrt{x_1^2+\cdots+x_4^2}+\frac{1}{2}\sqrt{x_5^2+\cdots+x_8^2}+\frac{1}{2}\sqrt{y_1^2+\cdots+y_4^2}+\frac{1}{2}\sqrt{y_5^2+\cdots+y_8^2}\\
\leq\;&\frac{1}{2}r+\frac{1}{2}r=r.
\end{aligned}$$

Para encontrarmos o volume, considere o problema com referência as coordenadas:

$$r_1=\sqrt{x_1^2+\cdots+x_4^2}\;\;,\;\;r_2=\sqrt{x_5^2+\cdots+x_8^2}.$$

Então a região $\mathcal{C}(r)$ é definida por $r_1+r_2\leq r$. Para cada ponto em distância radial r_1 da origem no espaço de dimensão 4 gerado pelas primeiras 4 x-coordenadas, existe uma região de volume $Vol(B_4(r-r_1))$ em $\mathcal{C}(r)$. Daí e do lema 3.22, temos que:

$$Vol(\mathcal{C}(r))=\int_{B_4(r)}Vol(B_4(r-r_1))=2\pi^2\int_{r_1=0}^{r}\frac{\pi^2}{2}(r-r_1)^4r_1^3\,dr_1\;,$$

e utilizando as técnicas de integração do cálculo, temos $Vol(\mathcal{C}(r))=\frac{\pi^4}{280}r^8$. ■

Lema 3.29 (Euler) *Se um inteiro algébrico que é soma de dois quadrados é dividido por um primo que é uma soma de dois quadrados, então o quociente é uma soma de dois quadrados.*

Demonstração. Suponha por exemplo que a^2+b^2 é divisível por p^2+q^2 e que p^2+q^2 é primo. Então:

$$p^2+q^2\mid(pb-aq)\cdot(pb+aq).$$

De fato, observe que:

$$\begin{aligned}
(pb-aq)\cdot(pb+aq)&=p^2b^2-a^2q^2=p^2b^2+p^2a^2-p^2a^2-a^2q^2\\
&=p^2(a^2+b^2)-a^2(p^2+q^2).
\end{aligned}$$

Como p^2+q^2 é primo, temos:

$$p^2+q^2\mid(pb-aq)\;\text{ ou }\;p^2+q^2\mid(pb+aq).$$

Suponha primeiro que $p^2+q^2 \mid (pb+aq)$. Observe ainda que:

$$(a^2+b^2)\cdot(p^2+q^2) = (ap-bq)^2+(aq+bp)^2 \implies p^2+q^2 \mid (ap-bq)^2;$$

portanto,

$$\frac{(a^2+b^2)\cdot(p^2+q^2)}{(p^2+q^2)^2} = \frac{a^2+b^2}{p^2+q^2}$$

é uma soma de dois quadrados.

O segundo caso, ou seja, $p^2+q^2 \mid (pb-aq)$ é feito de forma análoga, usando $(a^2+b^2)\cdot(q^2+p^2) = (aq-bp)^2+(ap+bq)^2$. ■

Teorema 3.30 *Para todo primo ρ de $I_{\mathbb{Q}(\sqrt{5})}$ existe uma unidade k e inteiros algébricos x, y, z, w tal que:*

$$k\rho = x^2+y^2+z^2+w^2, \quad \textit{onde } k, x, y, z, w \in I_{\mathbb{Q}(\sqrt{5})}.$$

Demonstração. A demonstração divide-se em casos como no teorema dos dois quadrados. Seja o primo ρ acima do primo p de $\mathbb{Z}$. Se p permanece inerte em $I_{\mathbb{Q}(\sqrt{5})}$ então o teorema segue trivialmente do correspondente teorema para inteiros racionais.

Se p ramifica, então ρ deve ser $\sqrt{5}$ vezes uma unidade, e já vimos que p possui uma representação como uma soma de dois quadrados.

Suponha que p se decompõe, então já vimos que $|\rho\cdot\overline{\rho}| = p$. Pelo lema 2.30 existem racionais inteiros a, b tal que:

$$a^2+b^2+1 \equiv 0 \bmod p \implies a^2+b^2+1 \equiv 0 \bmod \rho\ , \tag{3.20}$$

pois, $p \in \rho\cdot I_{\mathbb{Q}(\sqrt{5})}$. Seja S o $\mathbb{Z}$-módulo gerado pelos elementos do seguinte conjunto:

$$\left\{ \begin{array}{l} (1,1,0,0,a,a,b,b), (\varepsilon,\overline{\varepsilon},0,0,a\varepsilon,a\overline{\varepsilon},b\varepsilon,b\overline{\varepsilon}), \\ (0,0,1,1,b,b,-a,-a), (0,0,\varepsilon,\overline{\varepsilon},b\varepsilon,b\overline{\varepsilon},-a\varepsilon,-a\overline{\varepsilon}), \\ (0,0,0,0,\rho,\overline{\rho},0,0), (0,0,0,0,\varepsilon\rho,\overline{\varepsilon\rho},0,0), \\ (0,0,0,0,0,0,\rho,\overline{\rho}), (0,0,0,0,0,0,\varepsilon\rho,\overline{\varepsilon\rho}) \end{array} \right\}$$

Pelo lema 2.11 e a definição 2.16, temos:

$$\begin{aligned}
Vol(S) &= \left|\det\begin{pmatrix}
1 & \varepsilon & 0 & 0 & 0 & 0 & 0 & 0\\
1 & \overline{\varepsilon} & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & \varepsilon & 0 & 0 & 0 & 0\\
0 & 0 & 1 & \overline{\varepsilon} & 0 & 0 & 0 & 0\\
a & a\varepsilon & b & b\varepsilon & \rho & \varepsilon\rho & 0 & 0\\
a & a\overline{\varepsilon} & b & b\overline{\varepsilon} & \overline{\rho} & \overline{\varepsilon\rho} & 0 & 0\\
b & b\varepsilon & -a & -a\varepsilon & 0 & 0 & \rho & \varepsilon\rho\\
b & b\overline{\varepsilon} & -a & -a\overline{\varepsilon} & 0 & 0 & \overline{\rho} & \overline{\varepsilon\rho}
\end{pmatrix}\right| \\
&= \left|\frac{1}{\overline{\varepsilon}^2}\cdot\frac{1}{\overline{\varepsilon\rho}^2}\cdot\overline{\varepsilon}^2\cdot\overline{\varepsilon\rho}^2\cdot(\overline{\varepsilon}-\varepsilon)^2\cdot(\rho\cdot\overline{\varepsilon\rho}-\overline{\rho}\cdot\varepsilon\rho)^2\right| \\
&= \left|(\overline{\varepsilon}-\varepsilon)^4\cdot\rho^2\cdot\overline{\rho}^2\right| = \left|(-\sqrt{5})^4\cdot\rho^2\cdot\overline{\rho}^2\right| = \left|25\cdot\rho^2\cdot\overline{\rho}^2\right| \\
&= \left|25(\rho\cdot\overline{\rho})^2\right| = 25p^2 \neq 0.
\end{aligned}$$

Portanto, S é um reticulado em $\mathbb{R}^8$. Um elemento genérico deste reticulado é dado por:

$$\begin{aligned}
&x\cdot(1,1,0,0,a,a,b,b) + y\cdot(\varepsilon,\overline{\varepsilon},0,0,a\varepsilon,a\overline{\varepsilon},b\varepsilon,b\overline{\varepsilon})\\
&+ z\cdot(0,0,1,1,b,b,-a,-a) + w\cdot(0,0,\varepsilon,\overline{\varepsilon},b\varepsilon,b\overline{\varepsilon},-a\varepsilon,-a\overline{\varepsilon})\\
&+ r\cdot(0,0,0,0,\rho,\overline{\rho},0,0) + s\cdot(0,0,0,0,\varepsilon\rho,\overline{\varepsilon\rho},0,0)\\
&+ t\cdot(0,0,0,0,0,0,\rho,\overline{\rho}) + u\cdot(0,0,0,0,0,0,\varepsilon\rho,\overline{\varepsilon\rho}),
\end{aligned}$$

com $x,y,z,w,r,s,t,u\in\mathbb{Z}$. Ou ainda:

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

onde $\alpha,\beta,\mu,\nu\in I_{_{\mathbb{Q}(\sqrt{5})}}$.

O teorema de Minkowski (corolário 2.23) usando $\mathcal{C}(r)$ em $\mathbb{R}^8$, exigirá um parâmetro r tal que:

$$\frac{\pi^4}{280}r^8 \geq 2^8\times 25p^2 \implies r^8 \geq \frac{2^8\times 25\times 280}{\pi^4}\cdot p^2 \implies r^4 \geq \frac{2^4\times 10\times\sqrt{70}}{\pi^2}\cdot p.$$

Basta tomarmos $r=(3,42)\cdot p^{\frac{1}{4}}$. Um ponto do reticulado que está em $\mathcal{C}(r)$ é da forma $(\alpha,\overline{\alpha},\beta,\overline{\beta},\gamma,\overline{\gamma},\delta,\overline{\delta})$ tal que:

$$r_1=\sqrt{\alpha^2+\beta^2+\gamma^2+\delta^2}\ ,\ r_2=\sqrt{\overline{\alpha}^2+\overline{\beta}^2+\overline{\gamma}^2+\overline{\delta}^2}$$

e

$$r_1+r_2\leq r=(3,42)\cdot p^{\frac{1}{4}} \tag{3.21}$$

Utilizando (3.20), observe que:

$$\begin{aligned}
\alpha^2+\beta^2+\gamma^2+\delta^2 &= \alpha^2+\beta^2+(a\alpha+b\beta+\mu\rho)^2+(b\alpha-a\beta+\nu\rho)^2\\
&= \alpha^2+\beta^2+a^2\alpha^2+2ab\alpha\beta+b^2\beta^2+2\mu(a\alpha+b\beta)\rho+\mu^2\rho^2\\
&\quad +b^2\alpha^2-2ab\alpha\beta+a^2\beta^2+2\nu(b\alpha-a\beta)\rho+\nu^2\rho^2\\
&= (1+a^2+b^2)\alpha^2+(1+a^2+b^2)\beta^2+t\rho\\
&= \underbrace{(1+a^2+b^2)}_{\equiv 0 \bmod \rho}(\alpha^2+\beta^2)+t\rho,\ \text{com}\ t\in I_{\mathbb{Q}(\sqrt{5})}
\end{aligned}$$

Daí, $\alpha^2+\beta^2+\gamma^2+\delta^2 \equiv 0 \bmod \rho$. Portanto, existe $k \in I_{\mathbb{Q}(\sqrt{5})}$ tal que:

$$\alpha^2+\beta^2+\gamma^2+\delta^2 = k\rho \ \text{ e } \ \overline{\alpha}^2+\overline{\beta}^2+\overline{\gamma}^2+\overline{\delta}^2 = \overline{k\rho}. \tag{3.22}$$

Utilizando (3.21), temos:

$$\sqrt{k\rho}+\sqrt{\overline{k\rho}} \leq (3,42)\cdot p^{\frac{1}{4}}.$$

Pelo que anteriormente vimos,

$$\left(\sqrt{k\rho}-\sqrt{\overline{k\rho}}\right)^2 \geq 0 \implies k\rho-2\sqrt{k\rho}\cdot\sqrt{\overline{k\rho}}+\overline{k\rho} \geq 0 \implies k\rho+\overline{k\rho} \geq 2\sqrt{k\rho}\cdot\sqrt{\overline{k\rho}}.$$

Também,

$$\left(\sqrt{k\rho}+\sqrt{\overline{k\rho}}\right)^2 = k\rho+\overline{k\rho}+2\sqrt{k\rho}\cdot\sqrt{\overline{k\rho}} \geq 4\sqrt{k\rho\cdot\overline{k\rho}}.$$

Como $k\rho$ é totalmente positivo, temos:

$$\sqrt{k\rho}+\sqrt{\overline{k\rho}} \geq 2\sqrt{\sqrt{k\rho\cdot\overline{k\rho}}}.$$

Podemos concluir que:

$$2\sqrt{\sqrt{k\rho\cdot\overline{k\rho}}} \leq \sqrt{k\rho}+\sqrt{\overline{k\rho}} \leq (3,42)\cdot p^{\frac{1}{4}} \implies \left|k\rho\cdot\overline{k\rho}\right|^{\frac{1}{4}} \leq \left(\frac{3,42}{2}\right)\cdot p^{\frac{1}{4}};$$

daí, temos:

$$p^{\frac{1}{4}}\cdot\left|k\cdot\overline{k}\right|^{\frac{1}{4}} \leq (1,71)\cdot p^{\frac{1}{4}} \implies \left|k\cdot\overline{k}\right| \leq (1,71)^4 \implies \left|k\cdot\overline{k}\right| \leq 8,55. \tag{3.23}$$

Já vimos anteriormente que $\mathcal{N}(k) = k\cdot\overline{k}$ é um quadrado módulo 5, não podendo portanto ser congruente a 2 ou 3 módulo 5. Donde temos as possibilidades $\pm 1, \pm 4, \pm 5$ e ± 6 para $\mathcal{N}(k)$. Todavia 2 e 3 permanecem primos em $I_{\mathbb{Q}(\sqrt{5})}$. Se,

$$\mathcal{N}(k) = \pm 6 = \pm 3\cdot 2 = k\cdot\overline{k} \implies 3 \mid k \ \text{ ou } \ 3 \mid \overline{k} \implies 3 \mid k, \overline{k}\ ;$$

portanto:

$$k \cdot \overline{k} = 3t \cdot 3\overline{t} = 9 \cdot t \cdot \overline{t} \implies 9 \mid k \cdot \overline{k} \ ;$$

e isto é uma contradição em virtude de (3.23).

Se,

$$\mathcal{N}(k) = \pm 4 = \pm 2 \cdot 2 = k \cdot \overline{k} \implies 2 \mid k \text{ ou } 2 \mid \overline{k} \implies 2 \mid k, \overline{k} \ ;$$

ou seja:

$$k = 2 \cdot m \text{ com } m \in I_{\mathbb{Q}(\sqrt{5})} \implies \overline{k} = 2 \cdot \overline{m} \ ;$$

então:

$$\pm 4 = 2m \cdot 2\overline{m} = 4 \cdot m \cdot \overline{m} \implies m \cdot \overline{m} = \pm 1 \implies \mathcal{N}(m) = \pm 1;$$

segue que m é uma unidade. Portanto, k e $\overline{k}$ serão 2 vezes uma unidade. Tomando a equação (3.22) módulo 2, temos:

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 \bmod 2.$$

Se duas das variáveis são congruentes módulo 2, digamos $\alpha \equiv \beta \bmod 2$, então:

$$\alpha - \beta \equiv 0 \bmod 2 \implies (\alpha - \beta)^2 \equiv 0 \bmod 2 \implies \alpha^2 - 2\alpha\beta + \beta^2 \equiv 0 \bmod 2 \ ;$$

segue que:

$$\alpha^2 + \beta^2 \equiv 0 \bmod 2 \implies \gamma^2 + \delta^2 \equiv 0 \bmod 2.$$

Daí, $\frac{\alpha \pm \beta}{2}$ e $\frac{\gamma \pm \delta}{2}$ são inteiros algébricos. Pelo lema 3.22, temos:

$$\begin{aligned} \left(\frac{\alpha+\beta}{2}\right)^2 + \left(\frac{\alpha-\beta}{2}\right)^2 + \left(\frac{\gamma+\delta}{2}\right)^2 + \left(\frac{\gamma-\delta}{2}\right)^2 &= \frac{\alpha^2+\beta^2}{2} + \frac{\gamma^2+\delta^2}{2} \\ &= \frac{k}{2} \cdot \rho = m \cdot \rho. \end{aligned}$$

Portanto, ρ vezes uma unidade é uma soma de quatro quadrados.

O outro caso é se os valores das quatro variáveis α, β, γ e δ são todos distintos módulo 2. Considere o corpo:

$$\frac{I_{\mathbb{Q}(\sqrt{5})}}{(2)} = \{a + b\varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} : a, b \in \mathbb{Z}\}$$

Este corpo é finito de ordem $2^2 = 4$. Temos as classes:

$$\begin{cases} 2m + 2n\varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} = 0 + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} \\ 2m + 1 + 2n\varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} = 1 + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} \\ 2m + (2n+1)\varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} = \varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} \\ 2m + 1 + (2n+1)\varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} = 1 + \varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} = \overline{\varepsilon} + \varepsilon + \varepsilon + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} = \overline{\varepsilon} + 2 \cdot I_{\mathbb{Q}(\sqrt{5})} \ ; \end{cases}$$

ou seja, $\{0, 1, \varepsilon, \overline{\varepsilon}\}$ são as classes residuais. Os quatro valores podem portanto ser escritos como:

$$2\nu_1 + 0, 2\nu_2 + 1, 2\nu_3 + \varepsilon \text{ e } 2\nu_4 + \overline{\varepsilon},$$

onde todos os ν's são inteiros algébricos. Tomando a soma dos quatro quadrados dados, temos:

$$\begin{aligned}(2\nu_1)^2 + (2\nu_2 + 1)^2 + (2\nu_3 + \varepsilon)^2 + (2\nu_4 + \overline{\varepsilon})^2 &= 4\nu_1^2 + 4\nu_2^2 + 4\nu_2 + 1 + 4\nu_3^2 + 4\nu_3\varepsilon + \\ &\quad + \varepsilon^2 + 4\nu_4^2 + 4\nu_4\overline{\varepsilon} + \overline{\varepsilon}^2 \\ &\equiv 1 + \varepsilon^2 + \overline{\varepsilon}^2 \bmod 4;\end{aligned}$$

mas,

$$1 + \varepsilon^2 + \overline{\varepsilon}^2 = 1 + \left(\frac{1+\sqrt{5}}{2}\right)^2 + \left(\frac{1-\sqrt{5}}{2}\right)^2 = 1 + \frac{3+\sqrt{5}}{2} + \frac{3-\sqrt{5}}{2} = 1 + 3 = 4.$$

Portanto,

$$(2\nu_1)^2 + (2\nu_2 + 1)^2 + (2\nu_3 + \varepsilon)^2 + (2\nu_4 + \overline{\varepsilon})^2 \equiv 1 + \varepsilon^2 + \overline{\varepsilon}^2 \bmod 4 \equiv 0 \bmod 4.$$

Segue então que:

$$k\rho = 4\varphi \implies 2m\rho = 4\varphi \implies m\rho = 2\varphi \text{ com } \varphi \in I_{\mathbb{Q}(\sqrt{5})}.$$

Logo, $\rho = 2n$ com n uma unidade. Como 2 é soma de quatro quadrados, então o resultado segue.

Finalmente o caso de $\mathcal{N}(k) = \pm 5$. Neste caso, pelo teorema 3.16, k é primo e deve ser igual a $\sqrt{5}$ vezes uma unidade. Daí,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv 0 \bmod \sqrt{5}.$$

Como $\sqrt{5}$ é primo em $I_{\mathbb{Q}(\sqrt{5})}$, então $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(\sqrt{5})}$ é um corpo; e mais:

$$\mathfrak{f}((\sqrt{5})) = \left[\frac{I_{\mathbb{Q}(\sqrt{5})}}{(\sqrt{5})} : \mathbb{F}_5\right],$$

onde 5 é o único primo de $\mathbb{Z}$ em $(\sqrt{5})$. Temos ainda que:

$$\mathfrak{N}((\sqrt{5})) = \left|\mathcal{N}(\sqrt{5})\right| = 5 = 5^{\mathfrak{f}} \implies \mathfrak{f} = 1 \implies \frac{I_{\mathbb{Q}(\sqrt{5})}}{(\sqrt{5})} \simeq \frac{\mathbb{Z}}{5\mathbb{Z}}.$$

Como os quadrados em $\frac{\mathbb{Z}}{5\mathbb{Z}}$ são apenas $0, 1$ e -1, então para termos soma de quatro quadrados igual a zero, devemos ter:

1^o) Todos os quatro são nulos;

2^o) Pares de quadrados não nulos com um -1 cancelando cada quadrado que é igual a 1.

Em qualquer um dos casos nós podemos quebrar os quatro quadrados em dois pares onde a soma dos quadrados em cada par é zero.

Voltando a $\frac{I_{\mathbb{Q}(\sqrt{5})}}{(\sqrt{5})}$ via isomorfismo, temos os quatro quadrados quebrados em dois pares, cada um dos quais a soma é congruente a 0 módulo $\sqrt{5}$.

Nós mostramos no teorema 3.25 que $\varepsilon\sqrt{5}$ é soma de dois quadrados. Aplicando o lema de Euler (lema 3.29) para a equação:

$$\frac{\alpha^2+\beta^2}{\varepsilon\sqrt{5}}+\frac{\gamma^2+\delta^2}{\varepsilon\sqrt{5}}=\left(\frac{k}{\varepsilon\sqrt{5}}\right)\rho,$$

temos que ρ vezes uma unidade é uma soma de quatro quadrados. ■

Teorema 3.31 (Götzky) *Todo inteiro totalmente positivo de $I_{\mathbb{Q}(\sqrt{5})}$ é a soma de quatro quadrados de inteiros deste anel.*

Demonstração. Desde que $I_{\mathbb{Q}(\sqrt{5})}$ é um domínio de ideais principais, e um domínio de fatoração única, nós podemos escrever um inteiro totalmente positivo arbitrário α como um produto de primos; ou seja:

$$\alpha=\rho_1\cdot\rho_2\cdot\cdots\cdot\rho_m. \tag{3.24}$$

Se ρ_1 é totalmente positivo ($\rho_1,\overline{\rho_1}>0$), divida ambos os lados de (3.24) por ρ_1, ou seja:

$$\rho_1^{-1}\cdot\alpha=\rho_2\cdot\cdots\cdot\rho_m\ ,$$

onde nós temos do lado esquerdo um inteiro totalmente positivo e do lado direito um produto de primos.

Se $\rho_1,\overline{\rho_1}<0$, então $-\rho_1,\overline{-\rho_1}>0$ e $(-\rho_1)$ é totalmente positivo. Portanto,

$$\alpha=(-\rho_1)\cdot(-\rho_2)\cdot\rho_3\cdot\cdots\cdot\rho_m\implies(-\rho_1)^{-1}\cdot\alpha=(-\rho_2)\cdot\rho_3\cdot\cdots\cdot\rho_m\ ,$$

sendo do lado esquerdo um inteiro totalmente positivo e do lado direito um produto de primos.

Se ρ_1 e $\overline{\rho_1}$ tem sinais contrários, ou seja:

1^o) $\rho_1 > 0$ e $\overline{\rho_1} < 0$, então:

$$\varepsilon \cdot \rho_1 > 0 \text{ e } \overline{\varepsilon \cdot \rho_1} = \overline{\varepsilon} \cdot \overline{\rho_1} > 0 \ ;$$

e portanto, $\varepsilon \cdot \rho_1$ é totalmente positivo e podemos escrever:

$$\alpha = (\varepsilon \cdot \rho_1) \cdot (\varepsilon^{-1} \cdot \rho_2) \cdot \rho_3 \cdot \cdots \cdot \rho_m \implies (\varepsilon \cdot \rho_1)^{-1} \cdot \alpha = (\varepsilon^{-1} \cdot \rho_2) \cdot \rho_3 \cdot \cdots \cdot \rho_m.$$

2^o) $\rho_1 < 0$ e $\overline{\rho_1} > 0$, então:

$$-\varepsilon \cdot \rho_1 > 0 \text{ e } \overline{-\varepsilon \cdot \rho_1} = -\overline{\varepsilon} \cdot \overline{\rho_1} > 0 \ ;$$

e portanto, $-\varepsilon \cdot \rho_1$ é totalmente positivo e podemos escrever:

$$\alpha = (-\varepsilon \cdot \rho_1) \cdot (-\varepsilon^{-1} \cdot \rho_2) \cdot \rho_3 \cdot \cdots \cdot \rho_m \implies (-\varepsilon \cdot \rho_1)^{-1} \cdot \alpha = (-\varepsilon^{-1} \cdot \rho_2) \cdot \rho_3 \cdot \cdots \cdot \rho_m$$

Portanto, em todos os casos ficamos com um inteiro totalmente positivo do lado esquerdo igual a um produto de $m-1$ primos do lado direito. Procedendo por indução até que exista apenas um primo do lado direito, este será portanto totalmente positivo. Daí, podemos escrever α como um produto de primos totalmente positivos.

Dado algum primo ρ presente na fatoração de α, existe, pelo teorema 3.30, uma unidade k tal que $k\rho$ é soma de quatro quadrados. Daí, $k\rho$ e ρ são totalmente positivos. Com tudo,

$$k\rho = \mu^2 + \beta^2 + \gamma^2 + \delta^2 \implies \overline{k\rho} = \overline{k}\overline{\rho} = (\overline{\mu})^2 + (\overline{\beta})^2 + (\overline{\gamma})^2 + (\overline{\delta})^2.$$

Podemos então concluir que $k, \overline{k} > 0$, ou seja, k é uma unidade totalmente positiva.

Como todas as unidades de $I_{\mathbb{Q}(\sqrt{5})}$ são, em virtude do teorema 3.14, da forma $\pm\varepsilon^n$ e $\varepsilon > 0$ enquanto que $\overline{\varepsilon} < 0$, então $k = \varepsilon^{2n}$. Portanto:

$$\varepsilon^{2n} \cdot \rho = \mu^2 + \beta^2 + \gamma^2 + \delta^2 \implies \rho = (\mu\varepsilon^{-n})^2 + (\beta\varepsilon^{-n})^2 + (\gamma\varepsilon^{-n})^2 + (\delta\varepsilon^{-n})^2.$$

Portanto, ρ é soma de quatro quadrados de inteiros de $I_{\mathbb{Q}(\sqrt{5})}$. Utilizando a identidade de Lagrange(lema 1.6) para números reais, temos que α pode ser escrito como soma de quatro quadrados. ■

Apêndice A

Resultados Básicos

Neste capítulo apresentaremos alguns resultados, que serão amplamente utilizados em nossa dissertação e, de forma fundamental, nos ajudarão na compreensão da mesma. Em toda esta dissertação a palavra anel significa, salvo menção explícita em contrário, anel comutativo com unidade. [4, 8, 9].

A.1 O Anel dos Inteiros Algébricos

A noção de inteiro algébrico, bem como a de inteiro algébrico totalmente positivo são fundamentais em nossa dissertação. Nesta seção apresentaremos estes conceitos, bem como o anel dos inteiros algébricos e suas propriedades.

Por um *número algébrico* entendemos qualquer $\alpha \in \mathbb{C}$ que é algébrico sobre $\mathbb{Q}$. Chamamos de *corpo de números algébricos* a qualquer extensão finita L de $\mathbb{Q}$, não necessariamente contida em $\mathbb{C}$.

Definição A.1 *Sejam S um anel e R um subanel de S. Um elemento $\alpha \in S$ é* inteiro sobre R *se existir um polinômio mônico $f \in R[x]$ tal que $f(\alpha) = 0$. Em particular, todo elemento de R é inteiro sobre R.*

No caso $S = \mathbb{C}$, $R = \mathbb{Z}$, os números inteiros sobre $\mathbb{Z}$ são chamados *inteiros algébricos.*

Exemplo A.2 *Os números $i = \sqrt{-1}, \sqrt[5]{2}$ são inteiros algébricos, pois são raízes, respectivamente, dos polinômios $x^2 + 1, x^5 - 2 \in \mathbb{Z}[x]$.*

Definição A.3 *Um inteiro algébrico α é* totalmente positivo *se, e somente se, todas as raízes de $f_{\alpha, L|\mathbb{Q}}$ são positivas.*

Exemplo A.4 *Se* $\alpha = \frac{3+\sqrt{5}}{2}$*, então* $f_{\alpha,L|\mathbb{Q}}(x) = x^2 - 3x + 1$*, cujas raízes são* α *e* $\overline{\alpha} = \frac{3-\sqrt{5}}{2}$ *que são ambas positivas.*

Teorema A.5 *Para qualquer* $\alpha \in S$ *as seguintes condições são equivalentes:*

(i) α *é inteiro sobre* R*.*

(ii) $R[\alpha]$ *é um* R*-módulo finitamente gerado.*

(iii) *Existe um subanel* S' de S *que é um* R*-módulo finitamente gerado e tal que* $\alpha \in S'$*.*

(iv) *Existe um* R*-módulo finitamente gerado* M *tal que* $\alpha \cdot M \subseteq M$ *e que* $\gamma \cdot M \neq \{0\}$ *para todo* $\gamma \in R[\alpha] \setminus \{0\}$*.*

Demonstração. (i) $\Longrightarrow$ (ii): α é raiz de $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x]$. Então,

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0 \implies \alpha^n = -a_1\alpha^{n-1} - \cdots - a_n. \tag{A.1}$$

Considere o conjunto:

$$M = R + R \cdot \alpha + \cdots + R \cdot \alpha^{n-1};$$

obviamente $M \subseteq R[\alpha]$. Supondo que $1, \alpha, \ldots, \alpha^{n-1+k} \in M$, o que é elementar para $k = 0$, temos em virtude de (A.1) que:

$$\begin{aligned} \alpha^{n-1+k+1} &= \alpha^{n+k} = \alpha^n \cdot \alpha^k = (-a_1\alpha^{n-1} - \cdots - a_n) \cdot \alpha^k \\ &= -a_1\alpha^{n+k-1} - a_2\alpha^{n+k-2} - \cdots - a_n\alpha^k \in M \ ; \end{aligned}$$

logo $M = R[\alpha]$.

(ii) $\Longrightarrow$ (iii): Basta tomarmos $S' = R[\alpha]$.

(iii) $\Longrightarrow$ (iv): Basta tomarmos $M = S'$, pois $\alpha \cdot S' \subseteq S'$ e $\gamma = \gamma \cdot 1 \in \gamma \cdot S'$.

(iv) $\Longrightarrow$ (i): Seja $\beta_1, \ldots, \beta_r$ um sistema de geradores de M. Como $\alpha \cdot M \subseteq M$, existem $a_{jk} \in R$ tais que:

$$\begin{cases} \alpha \cdot \beta_1 = a_{11}\beta_1 + a_{12}\beta_2 + \cdots + a_{1r}\beta_r \\ \alpha \cdot \beta_2 = a_{21}\beta_1 + a_{22}\beta_2 + \cdots + a_{2r}\beta_r \\ \vdots \\ \alpha \cdot \beta_r = a_{r1}\beta_1 + a_{r2}\beta_2 + \cdots + a_{rr}\beta_r \end{cases},$$

ou seja, $\beta_1, \ldots, \beta_r$ é uma solução do sistema homogêneo de equações lineares:

$$\begin{cases} (\alpha - a_{11})x_1 - a_{12}x_2 - \cdots - a_{1r}x_r = 0 \\ -a_{21}x_1 + (\alpha - a_{22})x_2 - \cdots - a_{2r}x_r = 0 \\ \vdots \\ -a_{r1}x_1 - a_{r2}x_2 - \cdots - a_{r(r-1)}x_{r-1} + (\alpha - a_{rr})x_r = 0 \end{cases}$$

Chamando de $\varepsilon_{jk} = \alpha \cdot \delta_{jk} - a_{jk} \in R[\alpha]$, podemos reescrever o sistema na forma:

$$\sum_{k=1}^{r} \varepsilon_{jk} \cdot x_k = 0 \ (j = 1, \ldots, r).$$

Temos que $\varepsilon = \det(\varepsilon_{jk}) \in R[\alpha]$ e existem $\varepsilon_{ij}^* \in R[\alpha]$ tais que:

$$\sum_{j=1}^{r} \varepsilon_{ij}^* \cdot \varepsilon_{jk} = \varepsilon \cdot \delta_{ik} \quad (i, k = 1, \ldots, r).$$

Resulta que,

$$0 = \sum_{j,k=1}^{r} \varepsilon_{ij}^* \cdot \varepsilon_{jk} \cdot \beta_k = \sum_{k=1}^{r} \varepsilon \cdot \delta_{ik} \cdot \beta_k = \varepsilon \cdot \beta_i \ (i = 1, \ldots, r);$$

logo $\varepsilon \cdot M = \{0\}$, e assim $\varepsilon = 0$. Podemos concluir que α é raiz do polinômio mônico $\det(x \cdot \delta_{jk} - a_{jk}) \in R[x]$; logo α é inteiro sobre R. ■

Corolário A.6 *Se $\alpha_1, \ldots, \alpha_m \in S$ forem inteiros sobre R então $R[\alpha_1, \ldots, \alpha_m]$ será um R-módulo finitamente gerado.* ■

Considere o conjunto:

$$I_S(R) = \{a \in S : a \text{ é inteiro sobre } R\}.$$

Corolário A.7 ***a)*** *$I_S(R)$ é um subanel de S que contém R.*

b) *Todo subanel S' de S que é um R-módulo finitamente gerado, está contido em $I_S(R)$.*

Demonstração. a) Obviamente, pela definição A.1 $R \subseteq I_S(R) \subseteq S$. Sejam $\alpha, \beta \in I_S(R)$; então:

$$\alpha - \beta, \alpha \cdot \beta \in R[\alpha, \beta] \ ,$$

e pelo corolário A.6 $R[\alpha, \beta]$ é um R-módulo finitamente gerado; logo, pelo teorema A.5 temos:

$$\alpha - \beta, \alpha \cdot \beta \in I_S(R).$$

Portanto, $I_S(R)$ é um subanel de S.

b) é uma conseqüência imediata do teorema A.5. ■

O anel $I_S(R)$ é chamado *o fecho inteiro* de R em S. Quando $I_S(R) = R$ diremos que R é *integralmente fechado* em S. Quando $I_S(R) = S$ diremos que S é *inteiro sobre* R.

Observação A.8 *No caso de corpos $S = L$ e $R = K$, $I_L(K)$ é um subcorpo de L denominado de* fecho algébrico *de K em L. Em particular, teremos que $I_L(K) = K$ se, e somente se, K for algebricamente fechado em L, e $I_L(K) = L$ se, e somente se, a extensão $L \mid K$ for algébrica.*

Definição A.9 *Seja $S = L$ um corpo de números algébricos. O anel $I_L(\mathbb{Z})$ é chamado o* anel dos inteiros algébricos *de L e será denotado por I_L.*

Corolário A.10 *Sejam S um subanel de T e R um subanel de S. As seguintes condições são equivalentes:*

(i) T é inteiro sobre S e S é inteiro sobre R.

(ii) T é inteiro sobre R.

Demonstração. (i) $\Longrightarrow$ (ii): Cada $\gamma \in T$ é raiz de um polinômio $x^m + \alpha_1 \cdot x^{m-1} + \cdots + \alpha_m \in S[x]$. Como γ é inteiro sobre $S' = R[\alpha_1, \ldots, \alpha_m]$, então pelo teorema A.5 $S'[\gamma]$ é um S'-módulo finitamente gerado. Pelo corolário A.6, S' é um R-módulo finitamente gerado. Resulta que $S'[\gamma]$ é um R-módulo finitamente gerado; logo, pelo teorema A.5, γ é inteiro sobre R. A implicação (ii) $\Longrightarrow$ (i) é imediata ■

Definição A.11 *Um domínio R é* integralmente fechado *se for integralmente fechado no seu corpo de frações $K = Q(R)$, isto é, se $I_K(R) = R$.*

Teorema A.12 *Todo domínio fatorial R é integralmente fechado no seu corpo de frações.*

Demonstração. Todo $x \in K = Q(R)$, $x \neq 0$ pode ser escrito na forma

$$x = a \cdot b^{-1},\ a, b \in R,\ \text{MDC}(a, b) = 1.$$

Se $x \in I_K(R)$, então existem $c_1, \ldots, c_m \in R$ tais que:

$$x^m + c_1 x^{m-1} + \cdots + c_m = 0 \tag{A.2}$$

Multiplicando a equação (A.2) por b^m, obtemos:

$$a^m + c_1 b a^{m-1} + \cdots + c_m b^m = 0 \implies b \mid a^m.$$

Como $\text{MDC}(a, b) = 1 \implies b \in U(R) \implies x \in R.$ ■

Teorema A.13 *Seja R um subanel do corpo L. Então:*

$$Q(I_L(R)) = (I_L(R))_{R\setminus\{0\}} = I_L(Q(R)).$$

Em particular, $Q(I_L(R)) = L$ se, e somente se, L for algébrico sobre $Q(R)$.

Demonstração. Seja $\gamma \in Q(I_L(R)) \implies \gamma = \alpha \cdot \beta^{-1}$ onde $\alpha, \beta \in I_L(R), \beta \neq 0$. Como $I_L(Q(R))$ é um subcorpo de L contendo $I_L(R)$, temos que $\gamma \in I_L(Q(R))$. Daí, existem $b_1, \ldots, b_m, c_1, \ldots, c_m \in R$ tais que:

$$\gamma^m + \frac{b_1}{c_1}\gamma^{m-1} + \cdots + \frac{b_m}{c_m} = 0, \text{ com } c_1, \ldots, c_m \neq 0. \tag{A.3}$$

Seja $d = c_1 \cdot c_2 \cdot \cdots \cdot c_m$. Multiplicando-se a equação (A.3) por $d \cdot d^{-1}$, temos:

$$\gamma^m + \underbrace{b_1 c_2 \cdots c_m}_{=a_1} d^{-1}\gamma^{m-1} + \cdots + \underbrace{b_m c_1 \cdots c_{m-1}}_{=a_m} d^{-1} = 0,$$

ou seja,

$$\gamma^m + a_1 d^{-1}\gamma^{m-1} + \cdots + a_m d^{-1} = 0, \text{ com } a_1, \ldots, a_m \in R. \tag{A.4}$$

Multiplicando a equação (A.4) por d^m, temos:

$$(d\gamma)^m + a_1(d\gamma)^{m-1} + \cdots + a_m d^{m-1} = 0 \implies d\gamma \in I_L(R);$$

portanto, $\gamma = \frac{d\gamma}{d} \in (I_L(R))_{R\setminus\{0\}}$. A inclusão $(I_L(R))_{R\setminus\{0\}} \subseteq Q(I_L(R))$ é óbvia. A última afirmação também é imediata. ■

Corolário A.14 *Seja L um corpo de números algébricos. Então, $Q(I_L) = (I_L)_{\mathbb{Z}\setminus\{0\}} = L$.*
■

Teorema A.15 *Seja R um subanel de L e seja $K = Q(R)$.*

a) Se f, g forem polinômios mônicos em $K[x]$ e $f \cdot g \in R[x]$, então $f, g \in I_K(R)[x]$.

b) Para qualquer $\gamma \in I_L(R)$ temos que $p_{\gamma|K} \in I_K(R)[x]$.

Demonstração. a) Existem $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n \in \Omega$(fecho algébrico de L) tais que:

$$f(x) = \prod_{i=1}^{m}(x - \alpha_i) \text{ e } g(x) = \prod_{j=1}^{n}(x - \beta_j).$$

Como $(f \cdot g)(\alpha_i), (f \cdot g)(\beta_j) = 0$ e $f \cdot g \in R[x]$ então, $\alpha_i, \beta_j \in I_\Omega(R)$; portanto os coeficientes de f e g estão em $I_\Omega(R) \cap K = I_K(R)$.

b) γ é raiz de um polinômio mônico $h \in R[x]$; logo existe um polinômio mônico $g \in K[x]$ tal que

$$h = p_{\gamma|K} \cdot g.$$

De a) resulta que $p_{\gamma|K} \in I_K(R)[x]$. ■

Corolário A.16 *Sejam R um domínio integralmente fechado, L uma extensão finita de $K = Q(R)$ e S um subanel de $I_L(R)$ que contém R. Para qualquer $\gamma \in S$, temos que:*

a) $p_{\gamma|K}, f_{\gamma,L|K} \in R[x]$ e $\mathcal{N}_{L|K}(\gamma), \mathcal{T}_{L|K}(\gamma) \in R$.

b) $\mathcal{N}_{L|K}(\gamma)$ *é um múltiplo de* γ *no anel* S.

c) $\gamma \in U(S) \iff \mathcal{N}_{L|K}(\gamma) \in U(R)$.

d) *Se* $\mathcal{N}_{L|K}(\gamma)$ *for irredutível em* R então γ *será irredutível em* S.

Demonstração. Suponha que $\gamma \neq 0$. a) Resulta do ítem b) do teorema A.15 e da igualdade $f_{\gamma,L|K} = p_{\gamma|K}^m$, onde $m = [L : K(\gamma)]$.

b) Pelo ítem a), temos:

$$f_{\gamma,L|K} = x^n + a_1 x^{n-1} + \cdots + a_n \in R[x] \text{ e } \mathcal{N}_{L|K}(\gamma) = (-1)^n \cdot a_n.$$

Mas,

$$f_{\gamma,L|K}(\gamma) = 0 \implies a_n = (-1)^{-1}(\gamma^n + a_1\gamma^{n-1} + \cdots + a_{n-1}\gamma),$$

e portanto:

$$\mathcal{N}_{L|K}(\gamma) = \gamma \cdot \underbrace{(-1)^{n-1} \cdot (\gamma^{n-1} + a_1\gamma^{n-2} + \cdots + a_{n-1})}_{\in S}$$

c) Se $\gamma \cdot \delta = 1$ com $\delta \in S$ então,

$$\mathcal{N}_{L|K}(\gamma \cdot \delta) = \mathcal{N}_{L|K}(\gamma) \cdot \mathcal{N}_{L|K}(\delta) = \mathcal{N}_{L|K}(1) = 1, \text{ com } \mathcal{N}_{L|K}(\delta) \in R$$

Por outro lado, se $\mathcal{N}_{L|K}(\gamma) \in U(R)$ então, existe $\beta \in R$ tal que,

$$(\mathcal{N}_{L|K}(\gamma)) \cdot \beta = 1.$$

Pelo ítem b) temos que,

$$\mathcal{N}_{L|K}(\gamma) = r \cdot \gamma \text{ com } r \in S \text{ ;}$$

portanto,

$$(r \cdot \gamma) \cdot \beta = 1 \implies \gamma \cdot (r \cdot \beta) = 1 \implies \gamma \in U(S).$$

d) Suponha que $\gamma = r \cdot s$ com $r, s \in S$ não unidades. Então, pela multiplicatividade da norma, temos:

$$\mathcal{N}_{L|K}(\gamma) = \mathcal{N}_{L|K}(r) \cdot \mathcal{N}_{L|K}(s),$$

e pelo ítem c) $\mathcal{N}_{L|K}(\gamma)$ é redutível. ■

Corolário A.17 *Sejam L um corpo de números algébricos e S um subanel de I_L. Para qualquer $\gamma \in S$ temos que:*

a) $p_{\gamma|\mathbb{Q}}, f_{\gamma,L|\mathbb{Q}} \in \mathbb{Z}[x]$ e $\mathcal{N}_{L|\mathbb{Q}}(\gamma), \mathcal{T}_{L|\mathbb{Q}}(\gamma) \in \mathbb{Z}$

b) $\mathcal{N}_{L|\mathbb{Q}}(\gamma)$ *é um múltiplo de* γ *no anel* S.

c) $\gamma \in U(S) \iff \left|\mathcal{N}_{L|\mathbb{Q}}(\gamma)\right| = 1$.

d) *Se* $\left|\mathcal{N}_{L|\mathbb{Q}}(\gamma)\right|$ *for um número primo* então γ *será irredutível em* S. ■

No que segue, R e S são domínios quaisquer com $R \subseteq S$.

Teorema A.18 *Seja o domínio S inteiro sobre R. Então:*

a) *Para qualquer ideal $\mathfrak{U}$ não-nulo de S, $\mathfrak{U} \cap R$ é um ideal não-nulo de R.*

b) $U(S) \cap R = U(R)$.

c) *S será um corpo se, e somente se, R for um corpo.*

d) *Um ideal primo $\mathfrak{P}$ de S será um ideal maximal de S se, e somente se, $\mathfrak{P} \cap R$ for um ideal maximal de R.*

Demonstração. a) Seja $\alpha \in \mathfrak{U} \neq 0$. Como S é inteiro sobre R, seja

$$x^n + a_1 x^{n-1} + \cdots + a_n$$

um polinômio em $R[x]$ de menor grau que tenha α como raiz, ou seja:

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0 \implies a_n = \underbrace{-\alpha^n - a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha}_{\in \mathfrak{U}} \neq 0,$$

ou seja, $a_n \in \mathfrak{U} \cap R$.

b) Obviamente $U(S) \cap R \supseteq U(R)$. Seja $u \in U(S) \cap R$; então $u^{-1} \in S$. Como S é inteiro sobre R, existem $c_1, \ldots, c_m \in R$ tais que:

$$u^{-m} + c_1 u^{-m+1} + \cdots + c_m = 0. \tag{A.5}$$

Multiplicando a equação (A.5) por u^{m-1}, obtemos:

$$u^{-1} + c_1 + c_2 u + \cdots + c_m u^{m-1} = 0 \implies u^{-1} = -(c_1 + \cdots + c_m u^{m-1}) \in R[u] \subseteq R\ ;$$

logo $u \in U(R)$.

c) Seja S um corpo. Então,

$$U(S) = S \setminus \{0\} \implies U(R) = U(S) \cap R = (S \setminus \{0\}) \cap R = R \setminus \{0\}.$$

Portanto, R é um corpo. Por outro lado, se S não for um corpo, então possuirá um ideal não-nulo $\mathfrak{U}$ com $1 \notin \mathfrak{U}$. Por a), o ideal $\mathfrak{U} \cap R$ de R é não-nulo; logo R não é um corpo.

d) Considere a aplicação:

$$\begin{array}{rccc} \varphi: & S & \longrightarrow & \frac{S}{\mathfrak{P}} \\ & s & \longmapsto & s + \mathfrak{P} \end{array},$$

φ é claramente um homomorfismo sobrejetor e $\varphi\,|_R$ é tal que

$$\ker(\varphi\,|_R) = \{a \in R : \varphi(a) = \overline{0}\} = \{a \in R : a \in \mathfrak{P}\} = \mathfrak{P} \cap R.$$

Pelo teorema do homomorfismo, temos $\frac{R}{\mathfrak{P} \cap R} \simeq \frac{R}{\mathfrak{P}}$. Observe ainda que $\frac{S}{\mathfrak{P}}$ é inteiro sobre $\frac{R}{\mathfrak{P}}$. Daí,

$$\mathfrak{P} \text{ é maximal} \iff \frac{S}{\mathfrak{P}} \text{ é corpo} \iff \frac{R}{\mathfrak{P} \cap R} \text{ é corpo} \iff \mathfrak{P} \cap R \text{ é maximal em } R;$$

e portanto o teorema está provado. ■

Corolário A.19 *Seja o domínio S inteiro sobre R. Se todo ideal primo não-nulo de R for maximal então todo ideal primo não-nulo de S será maximal.*

Demonstração. Seja $\mathfrak{P}$ um ideal primo não-nulo de S. Então, pela parte a) do teorema A.18, $\mathfrak{P} \cap R$ é um ideal primo não-nulo de R, logo maximal, por hipótese. Pelo ítem d) do teorema A.18, $\mathfrak{P}$ é um ideal maximal de S. ■

Corolário A.20 *Seja L um corpo de números algébricos. Então todo ideal primo não-nulo de I_L é um ideal maximal de I_L.* ■

A.2 Norma de Ideais

Nesta seção apresentaremos a norma de ideais que generaliza a norma absoluta $\left|\mathcal{N}_{L|\mathbb{Q}}\right|$. Esta será uma importante ferramenta no estudo da decomposição de cada número primo p no anel I_L.

Sejam R um anel e $\mathfrak{M}$ um ideal maximal de R. Diremos que um R-módulo M é *anulado* por $\mathfrak{M}$ se $c \cdot x = 0$ para quaisquer $c \in \mathfrak{M}$ e $x \in M$.

Proposição A.21 *Os R-módulos anulados por $\mathfrak{M}$ coincidem com os $\frac{R}{\mathfrak{M}}$-espaços.*

Em particular, para todo ideal $\mathfrak{a}$ de R, o R-módulo quociente $\frac{\mathfrak{a}}{(\mathfrak{M}\cdot\mathfrak{a})}$ é anulado por $\mathfrak{M}$ e, portanto, pode ser considerado como $\frac{R}{\mathfrak{M}}$-espaço.

Demonstração. Considere a operação externa $\frac{R}{\mathfrak{M}} \times M \longrightarrow M$ bem definida por:

$$(\overline{r}, x) \longmapsto r \cdot x \ \left(\overline{r} \in \frac{R}{\mathfrak{M}}, x \in M\right),$$

onde $r \in R$ é um representante qualquer de $\overline{r}$, pois, se $r_1 \equiv r_2 \mathrm{mod}(\mathfrak{M})$, então:

$$r_1 \cdot x - r_2 \cdot x = (r_1 - r_2) \cdot x = 0.$$

Com esta operação, M é claramente um $\frac{R}{\mathfrak{M}}$-espaço. Por outro lado, qualquer $\frac{R}{\mathfrak{M}}$-espaço N pode ser considerado como R-módulo, com a operação $R \times N \longrightarrow N$ definida por:

$$(r, y) \longmapsto (r + \mathfrak{M}) \cdot y \ (r \in R, y \in N);$$

considerado como R-módulo, N é anulado por $\mathfrak{M}$. ■

Lema A.22 *Sejam R um domínio de Dedekind, $\mathfrak{M}$ um ideal maximal de R e $\mathfrak{a}$ um ideal não-nulo de R. Então $\frac{\mathfrak{a}}{(\mathfrak{M}\cdot\mathfrak{a})}$ é um $\frac{R}{\mathfrak{M}}$-espaço de dimensão 1.* ■

No que se segue, seja L um corpo de números algébricos, de grau $[L:\mathbb{Q}]=n$. Seja I_L o anel dos inteiros algébricos de L. Como I_L é um domínio de Dedekind então, todo ideal primo não-nulo $\mathfrak{p}$ de I_L é um ideal maximal de I_L; logo $\frac{I_L}{\mathfrak{p}}$ é um corpo, chamado o *corpo de restos* de I_L módulo $\mathfrak{p}$.

Teorema A.23 *Seja $\mathfrak{p}$ um ideal primo não-nulo de I_L; então:*

a) *$\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$, sendo p o único número primo em $\mathfrak{p}$.*

b) *$\frac{I_L}{\mathfrak{p}}$ é uma extensão finita do corpo $\mathbb{F}_p$, de grau $[\frac{I_L}{\mathfrak{p}}:\mathbb{F}_p]\leq n$.*

Demonstração. a) Pelo teorema A.18, o ideal primo $\mathfrak{p}\cap\mathbb{Z}$ é não-nulo; logo é igual a $p\mathbb{Z}$ para algum número primo p. Obviamente, p é o único número primo em $\mathfrak{p}$.

b) Considere o homomorfismo $k: I_L \longrightarrow \frac{I_L}{\mathfrak{p}}$. A restrição $k|_{\mathbb{Z}}:\mathbb{Z}\longrightarrow\frac{I_L}{\mathfrak{p}}$ tem como núcleo $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$; pelo teorema do homomorfismo, temos:

$$\mathbb{F}_p=\frac{\mathbb{Z}}{p\mathbb{Z}}\simeq k(\mathbb{Z}).$$

Identificando $k(\mathbb{Z})$ com $\mathbb{F}_p$, este torna-se um subcorpo de $\frac{I_L}{\mathfrak{p}}$. Portanto, existe uma base integral $\beta_1,\ldots,\beta_n$ de L. Obviamente, $k(\beta_1),\ldots,k(\beta_n)$ é um sistema de geradores do $\mathbb{F}_p$-espaço $\frac{I_L}{\mathfrak{p}}$; logo $[\frac{I_L}{\mathfrak{p}}:\mathbb{F}_p]\leq n$. ■

Definição A.24 *O grau $[\frac{I_L}{\mathfrak{p}}:\mathbb{F}_p]$ será chamado* o grau de inércia *de $\mathfrak{p}$ e denotado por $\mathfrak{f}(\mathfrak{p})$.*

Definição A.25 *Seja $\mathfrak{a}$ um ideal não-nulo de I_L. Será denotado por $\mathfrak{N}(\mathfrak{a})$, e chamado* norma do ideal $\mathfrak{a}$*, o número (cardinal) dos elementos de $\frac{I_L}{\mathfrak{a}}$.*

Proposição A.26

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

b) *Para todo ideal não-nulo $\mathfrak{a}$ de I_L temos que $\mathfrak{N}(\mathfrak{a})\in\mathbb{N}\setminus\{0\}$; em particular, $\mathfrak{N}(\mathfrak{a})=1$ se, e somente se, $\mathfrak{a}=I_L$.*

c) *Para quaisquer ideais não-nulos $\mathfrak{a}$, $\mathfrak{b}$ de I_L vale $\mathfrak{N}(\mathfrak{a}\cdot\mathfrak{b})=\mathfrak{N}(\mathfrak{a})\cdot\mathfrak{N}(\mathfrak{b})$.*

Demonstração. a) De $[\frac{I_L}{\mathfrak{p}} : \mathbb{F}_p] = \mathfrak{f}$ decorre que existem $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_\mathfrak{f}}$ base de $\frac{I_L}{\mathfrak{p}}$. Portanto, para todo $\overline{w} \in \frac{I_L}{\mathfrak{p}}$, temos:

$$\overline{w} = \overline{a_1} \cdot \overline{x_1} + \cdots + \overline{a_\mathfrak{f}} \cdot \overline{x_\mathfrak{f}} \text{ com } \overline{a_1}, \ldots, \overline{a_\mathfrak{f}} \in \mathbb{F}_p.$$

Como $|\mathbb{F}_p| = p$, temos que existem p-possibilidades para cada $\overline{a_i}$ $(i = 1, \ldots, \mathfrak{f})$. Portanto,

$$\left|\frac{I_L}{\mathfrak{p}}\right| = p^\mathfrak{f} = \mathfrak{N}(\mathfrak{p}).$$

b) e c): Afirmamos que $\mathfrak{N}(\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r) = \mathfrak{N}(\mathfrak{p}_1) \cdot \cdots \cdot \mathfrak{N}(\mathfrak{p}_r)$ para qualquer produto de r ideais primos não-nulos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ de I_L. Sendo trivial para $r = 0$, suponhamos que a afirmação seja válida para qualquer produto de $r-1$ ideais primos não-nulos, sendo $r \geq 1$. Sejam:

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r \text{ e } \mathfrak{b} = \mathfrak{p}_2 \cdot \cdots \cdot \mathfrak{p}_r \ ;$$

então, $\mathfrak{a} = \mathfrak{p}_1 \cdot \mathfrak{b} \subseteq \mathfrak{b}$. Considere o homomorfismo:

$$\begin{array}{rccc} \varphi : & \frac{I_L}{\mathfrak{a}} & \longrightarrow & \frac{I_L}{\mathfrak{b}} \\ & x + \mathfrak{a} & \longmapsto & x + \mathfrak{b} \end{array},$$

φ é claramente sobrejetivo e seu núcleo é dado por:

$$\begin{aligned} \ker(\varphi) &= \left\{\overline{x} \in \frac{I_L}{\mathfrak{a}} : \varphi(\overline{x}) = \overline{0} \in \frac{I_L}{\mathfrak{b}}\right\} = \left\{\overline{x} \in \frac{I_L}{\mathfrak{a}} : x + \mathfrak{b} = \mathfrak{b}\right\} \\ &= \left\{\overline{x} \in \frac{I_L}{\mathfrak{a}} : x \in \mathfrak{b}\right\} = \frac{\mathfrak{b}}{\mathfrak{a}}. \end{aligned}$$

Pelo teorema do homomorfismo, temos que:

$$\frac{\frac{I_L}{\mathfrak{a}}}{\frac{\mathfrak{b}}{\mathfrak{a}}} \simeq \frac{I_L}{\mathfrak{b}}.$$

Pelo lema A.22, $\frac{\mathfrak{b}}{\mathfrak{a}}$ é um $\frac{I_L}{\mathfrak{p}_1}$-espaço de dimensão 1, logo consiste de $\mathfrak{N}(\mathfrak{p}_1)$ elementos. Como $\frac{I_L}{\mathfrak{b}}$, por hipótese, consiste de $\mathfrak{N}(\mathfrak{p}_2) \cdot \cdots \cdot \mathfrak{N}(\mathfrak{p}_r)$ elementos, concluímos que $\frac{I_L}{\mathfrak{a}}$ consiste de $\mathfrak{N}(\mathfrak{p}_1) \cdot \cdots \cdot \mathfrak{N}(\mathfrak{p}_r)$ elementos, ou seja:

$$\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{p}_1) \cdot \cdots \cdot \mathfrak{N}(\mathfrak{p}_r) \in \mathbb{N} \setminus \{0\}.$$

Em particular,

$$\mathfrak{N}(\mathfrak{a}) = 1 \iff r = 0 \iff \mathfrak{a} = I_L.$$

As afirmações b) e c) resultam então do fato de todo ideal não-nulo de I_L ser um produto de ideais não-nulos. ■

Corolário A.27 *Seja $\mathfrak{a}$ um ideal não-nulo de I_L. Então:*

a) *$\mathfrak{N}(\mathfrak{a}) \in \mathfrak{a}$, ou seja, o ideal principal $I_L \cdot \mathfrak{N}(\mathfrak{a})$ é um múltiplo de $\mathfrak{a}$.*

b) *Se $\mathfrak{N}(\mathfrak{a})$ for um número primo então $\mathfrak{a}$ será um ideal primo.*

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

Lema A.28 *Para todo $m \in \mathbb{N} \setminus \{0\}$ existe somente um número finito de ideais não-nulos $\mathfrak{a}$ de I_L tais que $\mathfrak{N}(\mathfrak{a}) = m$.* ■

O teorema seguinte relaciona a norma de ideais com o discriminante e mostra que ela generaliza a norma absoluta $\left|\mathcal{N}_{L|\mathbb{Q}}\right|$.

Teorema A.29

a) *Todo ideal não-nulo $\mathfrak{a}$ de I_L é um $\mathbb{Z}$-módulo livre de posto n, e para toda base $\alpha_1, \ldots, \alpha_n$ deste $\mathbb{Z}$-módulo temos que:*

$$disc_{L|\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = (\mathfrak{N}(\mathfrak{a}))^2 \cdot d_L.$$

b) *Para todo elemento não-nulo $\alpha \in I_L$ temos que:*

$$\mathfrak{N}(I_L \cdot \alpha) = \left|\mathcal{N}_{L|\mathbb{Q}}(\alpha)\right|.$$

Demonstração. a) Como I_L é um $\mathbb{Z}$-módulo livre, obtemos uma base integral $\varepsilon_1, \ldots, \varepsilon_n$ de L e números inteiros $a_1, \ldots, a_q$, $q \leq n$, tais que $a_1 \cdot \varepsilon_1, \ldots, a_q \cdot \varepsilon_q$ formem uma base do $\mathbb{Z}$-módulo livre $\mathfrak{a}$. Portanto:

$$\frac{I_L}{\mathfrak{a}} \simeq \frac{\mathbb{Z}}{a_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{a_q\mathbb{Z}} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{n-q}.$$

Como $\mathfrak{N}(\mathfrak{a})$ é finita pela proposição A.26, concluímos que:

$$n = q \text{ e } \mathfrak{N}(\mathfrak{a}) = |a_1| \cdot \cdots \cdot |a_n| = |a_1 \cdot \cdots \cdot a_n|.$$

Observe que:

$$a_j \cdot \varepsilon_j = \sum_{i=1}^{n} a_i \cdot \delta_{ij} \cdot \varepsilon_i \ , \forall j = 1, \ldots, n.$$

Logo,

$$\begin{aligned} disc_{L|\mathbb{Q}}(a_1 \cdot \varepsilon_1, \ldots, a_n \cdot \varepsilon_n) &= (\det(a_i \cdot \delta_{ij}))^2 \cdot disc_{L|\mathbb{Q}}(\varepsilon_1, \ldots, \varepsilon_n) \\ &= |a_1 \cdot \cdots \cdot a_n|^2 \cdot d_L = (\mathfrak{N}(\mathfrak{a}))^2 \cdot d_L. \end{aligned}$$

Toda base $\alpha_1, \ldots, \alpha_n$ do $\mathbb{Z}$-módulo $\mathfrak{a}$ escreve-se como:

$$\alpha_i = \sum_{j=1}^{n} c_{ij} \cdot (a_j \cdot \varepsilon_j), \text{ com } c_{ij} \in \mathbb{Z} \ (i, j = 1, \ldots, n) \text{ e } \det(c_{ij}) \in U(\mathbb{Z}) = \{1, -1\};$$

portanto,

$$disc_{L|\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = disc_{L|\mathbb{Q}}(a_1 \cdot \varepsilon_1, \ldots, a_n \cdot \varepsilon_n).$$

b) Suponhamos que $\beta_1, \ldots, \beta_n$ formem uma base integral de L. Então $\alpha \cdot \beta_1, \ldots, \alpha \cdot \beta_n$ formam uma base do ideal principal $I_L \cdot \alpha$, considerado como $\mathbb{Z}$-módulo; logo, por a)

$$disc_{L|\mathbb{Q}}(\alpha \cdot \beta_1, \ldots, \alpha \cdot \beta_n) = (\mathfrak{N}(I_L \cdot \alpha))^2 \cdot d_L.$$

Por outro lado, existem $a_{ij} \in \mathbb{Z}$ tais que:

$$\alpha \cdot \beta_i = \sum_{j=1}^{n} a_{ij} \cdot \beta_j \ (j = 1, \ldots, n);$$

segue então que:

$$disc_{L|\mathbb{Q}}(\alpha \cdot \beta_1, \ldots, \alpha \cdot \beta_n) = (\det(a_{ij}))^2 \cdot d_L \text{ com } \det(a_{ij}) = \mathcal{N}_{L|\mathbb{Q}}(\alpha).$$

Concluimos que $\mathfrak{N}(I_L \cdot \alpha) = \left|\mathcal{N}_{L|\mathbb{Q}}(\alpha)\right|$. ■

Corolário A.30 *Seja p um número primo e seja $I_L \cdot p = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}$ a fatoração de $I_L \cdot p$ em ideais primos distintos $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, com $e_1 \geq 1, \ldots, e_r \geq 1$. Então:*

a) *$\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ são os únicos ideais primos $\mathfrak{p}$ de I_L tais que $p \in \mathfrak{p}$.*

b) *$\sum_{j=1}^{r} e_j \cdot \mathfrak{f}_j = n$, onde $\mathfrak{f}_j$ é o grau de inércia de $\mathfrak{p}_j$ $(j = 1, \ldots, r)$.*

Demonstração. a) Obviamente $p \in \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r} \subseteq \mathfrak{p}_j$ para todo $j \in \{1, \ldots, r\}$. Por outro lado,

$$p \in \mathfrak{p} \implies I_L \cdot p \subset \mathfrak{p} \implies \mathfrak{p} \mid I_L \cdot p \ ;$$

logo, pela unicidade da fatoração,

$$\mathfrak{p} \in \{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}.$$

b) Pela proposição A.26 e pelo ítem b) do teorema A.29, concluímos que:

$$\mathfrak{N}(I_L \cdot p) = \prod_{j=1}^{r} (\mathfrak{N}(\mathfrak{p}_j))^{e_j} = \prod_{j=1}^{r} p^{e_j \cdot \mathfrak{f}_j} \text{ e } \mathfrak{N}(I_L \cdot p) = \left|\mathcal{N}_{L|\mathbb{Q}}(p)\right| = p^n,$$

ou seja:

$$p^{\sum_{j=1}^{r} e_j \cdot \mathfrak{f}_j} = p^n$$

e portanto, $\sum_{j=1}^{r} e_j \cdot \mathfrak{f}_j = n$. ■

A.3 Anéis de Frações de um Domínio

Nesta seção apresentaremos o anel de frações de um domínio R, bem como algumas propriedades que são preservadas na passagem de R ao seu anel de frações. Veremos também que se R e S são anéis com $R \subseteq S$, então a noção de anel de frações será útil para estudar a relação entre os ideais primos de R e os de S, no caso em que S é inteiro sobre R.

Sejam S um anel qualquer e R um subanel de S. Denotamos por $\mathfrak{I}$ (respectivamente $\mathcal{I}$) o conjunto de todos os ideais de R (respectivamente de S). Associando a cada $\mathfrak{a} \in \mathfrak{I}$ o ideal:

$$\mathfrak{a} \cdot S = \{a_1 \cdot \gamma_1 + \cdots + a_s \cdot \gamma_s : a_1, \ldots, a_s \in \mathfrak{a} \, ; \gamma_1, \ldots, \gamma_s \in S \, ; s \in \mathbb{N}\},$$

obtemos uma aplicação $\varepsilon : \mathfrak{I} \longrightarrow \mathcal{I}$, chamada a *extensão de ideais* (de R a S). O subconjunto $\varepsilon(\mathfrak{I})$ de $\mathcal{I}$ é chamado o *conjunto dos ideais estendidos*.

Por outro lado, associando a cada $\mathcal{U} \in \mathcal{I}$ a intersecção $\mathcal{U} \cap R$, obtemos uma aplicação $\rho : \mathcal{I} \longrightarrow \mathfrak{I}$, chamada a *restrição de ideais* (de S a R). O subconjunto $\rho(\mathcal{I})$ de $\mathfrak{I}$ é chamado o *conjunto dos ideais restritos*.

Seja M um subconjunto multiplicativo do domínio R. Denotaremos, salvo menção em contrário, por $\mathfrak{I}$ (respectivamente $\mathcal{I}$) o conjunto dos ideais de R (respectivamente de R_M).

Lema A.31 *a) Para todo $\mathfrak{U} \in \mathcal{I}$ temos que $(\mathfrak{U} \cap R) \cdot R_M = \mathfrak{U}$.*

b) *Para todo $\mathfrak{a} \in \mathfrak{I}$ temos que $\mathfrak{a} \cdot R_M = \{\frac{a}{m} : a \in \mathfrak{a}, m \in M\}$; em particular, $\mathfrak{a} \cdot R_M = R_M$ se, e somente se, $\mathfrak{a} \cap M \neq \varnothing$.*

Demonstração. a) Seja $\alpha \in \mathfrak{U}$, digamos $\alpha = \frac{c}{m}$, com $c \in R$, $m \in M$. Então, $m \cdot \alpha = c \in \mathfrak{U} \cap R$; logo $\alpha = c \cdot \left(\frac{1}{m}\right) \in (\mathfrak{U} \cap R) \cdot R_M$. Claramente, $(\mathfrak{U} \cap R) \cdot R_M \subset \mathfrak{U}$. Portanto, $(\mathfrak{U} \cap R) \cdot R_M = \mathfrak{U}$.

b) Observe que:

$$\begin{aligned}
\mathfrak{a} \cdot R_M &= \left\{ a_1 \cdot \frac{b_1}{m_1} + \cdots + a_s \cdot \frac{b_s}{m_s} : a_i \in \mathfrak{a}; b_i \in R; m_i \in M \right\} \\
&= \left\{ \begin{array}{c} \frac{a_1 \cdot b_1 \cdot m_2 \cdot \cdots \cdot m_s + \cdots + a_s \cdot b_s \cdot m_1 \cdot \cdots \cdot m_{s-1}}{m_1 \cdot m_2 \cdot \cdots \cdot m_s} : a_i \in \mathfrak{a}; b_i \in R; \\ m_i \in M \end{array} \right\} \\
&= \left\{ \begin{array}{c} \frac{a}{m} : a = \sum_{i=1}^{s} a_i \cdot b_i \cdot m_1 \cdot \cdots \cdot m_{i-1} \cdot m_{i+1} \cdot \cdots \cdot m_s \in \mathfrak{a} \text{ e} \\ m = m_1 \cdot \cdots \cdot m_s \in M \end{array} \right\}.
\end{aligned}$$

Se $\mathfrak{a} \cdot R_M = R_M$, então existem $a \in \mathfrak{a}$ e $m \in M$ tais que $\frac{a}{m} = 1$; logo $a = m \in \mathfrak{a} \cap M$. Por outro lado, se $m \in \mathfrak{a} \cap M$ então $1 = \frac{m}{m} \in \mathfrak{a} \cdot R_M \implies \mathfrak{a} \cdot R_M = R_M$. ■

Definição A.32 *Diremos que o ideal* $\mathfrak{a} \in \mathfrak{I}$ se perde em R_M *quando* $\mathfrak{a} \cdot R_M = R_M$.

Denotamos por $\mathcal{P}$ (respectivamente $\mathfrak{L}$) o conjunto de todos so ideais primos de R (respectivamente de R_M), e por $\mathcal{P}_M$ o conjunto $\{\mathfrak{p} \in \mathcal{P} : \mathfrak{p} \cap M = \varnothing\}$.

Teorema A.33 *a) Para todo* $\mathfrak{P} \in \mathfrak{L}$ *temos que* $\mathfrak{P} \cap R \in \mathcal{P}_M$ *e* $(\mathfrak{P} \cap R) \cdot R_M = \mathfrak{P}$.

b) *Para todo* $\mathfrak{p} \in \mathcal{P}_M$ *temos que* $\mathfrak{p} \cdot R_M \in \mathfrak{L}$ *e* $\mathfrak{p} \cdot R_M \cap R = \mathfrak{p}$.

c) *As aplicações* ε *e* ρ *induzem aplicações bijetivas, inversas entre si, entre* $\mathcal{P}_M$ *e* $\mathfrak{L}$.

Demonstração. a) Obviamente $\mathfrak{P} \cap R \in \mathcal{P}$ para qualquer $\mathfrak{P} \in \mathfrak{L}$. Pelo lema A.31, temos que:

$$(\mathfrak{P} \cap R) \cdot R_M = \mathfrak{P} \neq R_M \implies (\mathfrak{P} \cap R) \cap M = \varnothing \implies \mathfrak{P} \cap R \in \mathcal{P}_M.$$

b) Seja $\mathfrak{p} \in \mathcal{P}_M$; então pelo ítem b) do lema A.31, temos que $\mathfrak{p} \cdot R_M \neq R_M$.

Sejam $a, b \in R$ e $m, n \in M$ tais que $\left(\frac{a}{m}\right) \cdot \left(\frac{b}{n}\right) \in \mathfrak{p} \cdot R_M$. Ainda pelo ítem b) do lema A.31, existem $c \in \mathfrak{p}$ e $k \in M$ tais que:

$$\left(\frac{a}{m}\right) \cdot \left(\frac{b}{n}\right) = \frac{c}{k} \implies a \cdot b \cdot k = m \cdot n \cdot c \in \mathfrak{p}.$$

Como $k \notin \mathfrak{p}$ decorre que,

$$a \cdot b \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ ou } b \in \mathfrak{p} \implies \frac{a}{m} \in \mathfrak{p} \cdot R_M \text{ ou } \frac{b}{n} \in \mathfrak{p} \cdot R_M ;$$

portanto, $\mathfrak{p} \cdot R_M \in \mathfrak{L}$.

Todo $d \in \mathfrak{p} \cdot R_M \cap R$ é da forma $\frac{c}{m}$, onde $c \in \mathfrak{p}$ e $m \in M$; logo $m \cdot d = c$; de $m \notin \mathfrak{p}$ decorre que:

$$d \in \mathfrak{p} \implies \mathfrak{p} \cdot R_M \cap R = \mathfrak{p}.$$

c) é uma conseqüência de a) e b). ■

Corolário A.34 *Para todo $\mathfrak{p} \in \mathcal{P}_M$, o homomorfismo canônico $\frac{R}{\mathfrak{p}} \longrightarrow \frac{R_M}{\mathfrak{p} \cdot R_M}$ é injetivo. Ele será bijetivo (e, portanto, um isomorfismo) quando $\mathfrak{p}$ for um ideal maximal.* ■

Corolário A.35 *Seja $M = R \backslash \mathfrak{p}_0$, onde $\mathfrak{p}_0 \in \mathcal{P}$. Sob as aplicações ε e ρ, os ideais primos de R_M correspondem biunivocamente aos ideais primos de R que estão contidos em $\mathfrak{p}_0$. Em particular, $\mathfrak{p}_0 \cdot R_M$ é o único ideal maximal de R_M.* ■

Teorema A.36 *Sejam S um domínio, R um subanel de S e M um subconjunto multiplicativo de R. Então:*

$$(I_S(R))_M = I_{S_M}(R_M).$$

Demonstração. Todo $s \in R' = I_S(R)$ satisfaz uma igualdade:

$$s^k + a_1 \cdot s^{k-1} + \cdots + a_k = 0, \text{ com } a_1, \ldots, a_k \in R, \ k \in \mathbb{N};$$

logo,

$$\left(\frac{s}{m}\right)^k + \left(\frac{a_1}{m}\right) \cdot \left(\frac{s}{m}\right)^{k-1} + \cdots + \frac{a_k}{m^k} = 0 \text{ para qualquer } m \in M.$$

Portanto, todo elemento de R'_M está em S_M e é inteiro sobre R_M; logo $R'_M \subseteq I_{S_M}(R_M)$. Por outro lado, sejam $s \in S$ e $m \in M$ e suponhamos que $\frac{s}{m}$ seja inteiro sobre R_M, digamos:

$$\left(\frac{s}{m}\right)^l + \left(\frac{b_1}{m_1}\right) \cdot \left(\frac{s}{m}\right)^{l-1} + \cdots + \frac{b_l}{m_l} = 0, \text{ onde } b_i \in R, m_i \in M \text{ e } l \in \mathbb{N}.$$

Multiplicando a igualdade acima por $(m \cdot n)^l$, onde $n = m_1 \cdot \cdots \cdot m_l$, obtemos:

$$(s \cdot n)^l + c_1 \cdot (s \cdot n)^{l-1} + \cdots + c_l = 0, \text{ com } c_1, \ldots, c_l \in R;$$

logo, $s \cdot n \in I_S(R) = R'$, e $\frac{s}{m} = \frac{s \cdot n}{m \cdot n} \in R'_M$. ■

Corolário A.37 *Sejam S, R e M como no teorema A.36.*

a) *Se S for inteiro sobre R então S_M será inteiro sobre R_M.*

b) *Se R for integralmente fechado em S então R_M será integralmente fechado em S_M.*■

Lema A.38 *Se R for um domínio noetheriano então todo anel de frações de R também o será.*

Demonstração. Para todo $\mathfrak{U} \in \mathcal{I}$, o ideal $\mathfrak{U} \cap R \in \mathfrak{I}$ é finitamente gerado, digamos:

$$\mathfrak{U} \cap R = R \cdot a_1 + \cdots + R \cdot a_r \ ;$$

logo, $\mathfrak{U} = (\mathfrak{U} \cap R) \cdot R_M = R_M \cdot a_1 + \cdots + R_M \cdot a_r$ é finitamente gerado. ■

Teorema A.39 *Sejam R um domínio de Dedekind e M um subconjunto multiplicativo de R; então:*

a) *R_M é um domínio de Dedekind.*

Além disto, para todo ideal primo não-nulo $\mathfrak{p}$ de R tal que $\mathfrak{p} \cap M = \varnothing$, temos que:

b) *os corpos $\frac{R}{\mathfrak{p}}$ e $\frac{R_M}{\mathfrak{p} \cdot R_M}$ são canonicamente isomorfos;*

c) *$\mathfrak{p}^k \cdot R_M \cap R = \mathfrak{p}^k$ para todo $k \in \mathbb{N}$.*

Demonstração. a) Pelo lema A.38 e pelo ítem b) do corolário A.37, R_M é noetheriano e integralmente fechado. Seja $\mathfrak{P} \in \mathfrak{L}$, $\mathfrak{P} \neq (0)$. Pelo teorema A.33, $\mathfrak{P} \cap R$ é um ideal primo não-nulo e, portanto, um ideal maximal de R; logo $\mathfrak{P}$ é um ideal maximal de R_M.

b) Resulta do corolário A.34.

c) Seja $a \in \mathfrak{p}^k \cdot R_M \cap R$; pelo ítem b) do lema A.31 existem $b \in \mathfrak{p}^k$ e $m \in M$ tais que:

$$a = \frac{b}{m} \implies m \cdot a = b.$$

Como $\mathfrak{p}^k$ divide o ideal $b \cdot R$ e $\mathfrak{p}$ não divide $m \cdot R$, resulta que $\mathfrak{p}^k$ divide o ideal $a \cdot R$, logo $a \in \mathfrak{p}^k$. A inclusão inversa é óbvia. ■

Definição A.40 *Um ideal primo $\mathfrak{P}$ de S está acima de $\mathfrak{p}$ se $\mathfrak{P} \cap R = \mathfrak{p}$.*

Teorema A.41 *Sejam S um domínio, R um subanel de S tal que S seja inteiro sobre R, e $\mathfrak{p}$ um ideal primo de R. Então:*

a) *Para todo $\mathfrak{U} \in \mathcal{I}$ tal que $\mathfrak{U} \cap R \subseteq \mathfrak{p}$ existe um ideal primo $\mathfrak{P}$ de S, acima de $\mathfrak{p}$, tal que $\mathfrak{U} \subseteq \mathfrak{P}$.*

b) *Os ideais primos $\mathfrak{P}$ de S que estão acima de $\mathfrak{p}$ são os elementos maximais do conjunto* $\{\mathfrak{U} \in \mathcal{I} : \mathfrak{U} \cap R \subseteq \mathfrak{p}\}$. ■

Corolário A.42 *Sejam S, R e $\mathfrak{p}$ como no teorema A.41.*

a) (Teorema "lying-over") *Existe um ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.*

b) *Se $\mathfrak{P}_1$, $\mathfrak{P}_2$ forem ideais primos de S, acima de $\mathfrak{p}$ e tais que $\mathfrak{P}_1 \subseteq \mathfrak{P}_2$, então $\mathfrak{P}_1 = \mathfrak{P}_2$.*

c) (Teorema "going-up") *Sejam $\mathfrak{p}_0$ e $\mathfrak{P}_0$ ideais primos de R e S, respectivamente, tais que $\mathfrak{P}_0$ esteja acima de $\mathfrak{p}_0$ e $\mathfrak{p}_0 \subseteq \mathfrak{p}$. Então existe um ideal primo $\mathfrak{P}$ de S, acima de $\mathfrak{p}$, tal que $\mathfrak{P}_0 \subseteq \mathfrak{P}$.* ■

A.4 Decomposição de ideais primos

Dados um domínio de Dedekind R, uma extensão finita e separável L do corpo $K = Q(R)$ e $S = I_L(R)$, apresentaremos nesta seção, para os ideais primos não-nulos $\mathfrak{p}$ de R, a decomposição de $\mathfrak{p}$ em L, isto é, a fatoração do ideal estendido $\mathfrak{p} \cdot S$ em ideais primos $\mathfrak{P}$ de S.

Sejam R, S, K, L como definidos acima, $n = [L : K]$, $\mathfrak{p}$ um ideal primo não-nulo de R, e $\mathcal{I}$ o conjunto dos ideais de S.

Lema A.43 *Seja $\mathfrak{p} \cdot S = \mathfrak{P}_1^{e_1} \cdot \cdots \cdot \mathfrak{P}_r^{e_r}$, sendo $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ ideais primos de S distintos, e $e_1 \geq 1, \ldots, e_r \geq 1$. Então:*

a) *$r \geq 1$.*

b) *$\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ são os ideais primos que estão acima de $\mathfrak{p}$.*

c) $\{\mathfrak{U} \in \mathcal{I} : \mathfrak{U} \cap R = \mathfrak{p}\} = \{\mathfrak{P}_1^{d_1} \cdot \cdots \cdot \mathfrak{P}_r^{d_r} : 0 \leq d_i \leq e_i \ (i = 1, \ldots, r), d_1 + \cdots + d_r \geq 1\}$.

Demonstração. a) Como $\mathfrak{p}$ é um ideal restrito pela parte a) do corolário A.42, temos que:

$$\mathfrak{p} \cdot S \cap R = \mathfrak{p} \implies \mathfrak{p} \cdot S \neq S \ ;$$

portanto, $\mathfrak{p} \cdot S$ é divisível por algum ideal primo $\mathfrak{P}$, isto é, $r \geq 1$.

c) O conjunto à direita consiste dos ideais $\mathfrak{U} \in \mathcal{I}$, $\mathfrak{U} \neq S$, que dividem $\mathfrak{p} \cdot S$. Para todo $\mathfrak{U}$ deste tipo temos que:

$$\mathfrak{p} \subseteq \mathfrak{p} \cdot S \cap R \subseteq \mathfrak{U} \cap R \neq R \ ;$$

logo, $\mathfrak{p} = \mathfrak{U} \cap R$ devido à maximalidade de $\mathfrak{p}$. Por outro lado, de $\mathfrak{U} \cap R = \mathfrak{p}$ decorre que:

$$\mathfrak{U} \neq S \text{ e } \mathfrak{p} \cdot S = (\mathfrak{U} \cap R) \cdot S \subseteq \mathfrak{U},$$

logo $\mathfrak{U}$ divide $\mathfrak{p} \cdot S$.

b) é uma conseqüência imediata de c). ■

Lema A.44 *Para todo ideal $\mathfrak{U}$ de S tal que $\mathfrak{U} \cap R = \mathfrak{p}$, o $\frac{R}{\mathfrak{p}}$-espaço $\frac{S}{\mathfrak{U}}$ tem dimensão finita.*

Demonstração. S é um R-módulo finitamente gerado. As classes mod $\mathfrak{U}$ de um sistema de geradores deste R-módulo formam um sistema de geradores do $\frac{R}{\mathfrak{p}}$-espaço $\frac{S}{\mathfrak{U}}$ que, portanto, tem dimensão finita. ■

Observação A.45 *$\frac{R}{\mathfrak{p}}$ pode ser identificado com a imagem de R sob o homomorfismo canônico de S sobre $\frac{S}{\mathfrak{U}}$ e, portanto, pode ser considerado como subcorpo do anel $\frac{S}{\mathfrak{U}}$. Em particular, para cada ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$, o corpo $\frac{S}{\mathfrak{P}}$ pode ser considerado como uma extensão do corpo $\frac{R}{\mathfrak{p}}$.*

Definição A.46 *O grau $[\frac{S}{\mathfrak{P}} : \frac{R}{\mathfrak{p}}] = \dim\left(\frac{S}{\mathfrak{P}}\right)$ é chamado* grau de inércia *de $\mathfrak{P}$ e é denotado por $f(\mathfrak{P} \mid \mathfrak{p})$.*

Definição A.47 *O maior número e tal que $\mathfrak{P}^e$ divida $\mathfrak{p} \cdot S$ é chamado* o índice de ramificação *de $\mathfrak{P}$ e é denotado por $e(\mathfrak{P} \mid \mathfrak{p})$.*

Teorema A.48 (Igualdade Fundamental) *Sejam R um domínio de Dedekind, $S = I_L(R)$, onde L é uma extensão finita e separável de $K = Q(R)$, $\mathfrak{p}$ um ideal primo não-nulo de R e $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ os ideais primos de S que estão acima de $\mathfrak{p}$. Então:*

$$\sum_{i=1}^{r} e(\mathfrak{P}_i \mid \mathfrak{p}) \cdot f(\mathfrak{P}_i \mid \mathfrak{p}) = \dim\left(\frac{S}{\mathfrak{p} \cdot S}\right) = [L : K].$$

■

Observação A.49 *A igualdade fundamental permite vários tipos de decomposição de $\mathfrak{p}$; convém dar nomes aos casos extremos. Diremos que o ideal primo $\mathfrak{p}$ de R é:*

a) *totalmente decomposto em L, quando $r = n$, ou seja, $e(\mathfrak{P} \mid \mathfrak{p}) = f(\mathfrak{P} \mid \mathfrak{p}) = 1$ para todo ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.*

b) *totalmente inerte em L, quando $r = 1$ e $e(\mathfrak{P}_1 \mid \mathfrak{p}) = 1$, ou seja, $f(\mathfrak{P} \mid \mathfrak{p}) = n$ para algum ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.*

c) *totalmente ramificado em L, quando $r = 1$ e $f(\mathfrak{P}_1 \mid \mathfrak{p}) = 1$, ou seja, $e(\mathfrak{P} \mid \mathfrak{p}) = n$ para algum ideal primo $\mathfrak{P}$ de S que está acima de $\mathfrak{p}$.*

No caso $n = 2$, estes três casos são obviamente os únicos.

Nosso próximo resultado permite indicar explicitamente tal decomposição a partir da fatoração $\bmod \mathfrak{p} \cdot R[x]$ do polinômio minimal $p_{\beta|K}$, sendo β qualquer elemento em S tal que $S = R[\beta]$.

Para todo polinômio $F = \sum_{i=1}^{r} a_i x^i \in R[x]$ denotaremos por $\overline{F}$ o polinômio $\sum_{i=1}^{r} (a_i + \mathfrak{p}) \cdot x^i \in \left(\frac{R}{\mathfrak{p}}\right)[x]$ (sendo $\mathfrak{p}$ fixo).

Teorema A.50 *Suponhamos que $S = R[\beta]$. Seja $P = p_{\beta|K}$ e sejam $P_1, \ldots, P_r$ polinômios mônicos em $R[x]$ tais que $\overline{P} = \overline{P_1}^{e_1} \cdot \cdots \cdot \overline{P_r}^{e_r}$ seja a fatoração de $\overline{P}$ em polinômios irredutíveis distintos em $\left(\frac{R}{\mathfrak{p}}\right)[x]$. Então:*

a) *$\mathfrak{p} \cdot S = \mathfrak{P}_1^{e_1} \cdot \cdots \cdot \mathfrak{P}_r^{e_r}$, onde $\mathfrak{P}_j = \mathfrak{p} \cdot S + P_j(\beta) \cdot S$ $(j = 1, \ldots, r)$ são os ideais primos de S, distintos, acima de $\mathfrak{p}$; logo $e(\mathfrak{P}_j \mid \mathfrak{p}) = e_j$ $(j = 1, \ldots, r)$.*

b) *$\frac{S}{\mathfrak{P}_j} = \left(\frac{R}{\mathfrak{p}}\right)(\overline{\beta_j})$, sendo $\overline{\beta_j}$ uma raiz de $\overline{P_j}$; logo $f(\mathfrak{P}_j \mid \mathfrak{p}) = \partial P_j$ $(j = 1, \ldots, r)$.* ■

Corolário A.51 *Com a hipótese e as notações do teorema A.50 temos que:*

a) *$\mathfrak{p}$ será totalmente decomposto em L se, e somente se, $\overline{P}$ se fatora em $\left(\frac{R}{\mathfrak{p}}\right)[x]$ em fatores lineares distintos $x - (a_j + \mathfrak{p})$ $(j = 1, \ldots, n)$; neste caso $\mathfrak{p} \cdot S = \mathfrak{P}_1 \cdot \cdots \cdot \mathfrak{P}_n$, sendo $\mathfrak{P}_j = \mathfrak{p} \cdot S + (\beta - a_j) \cdot S$ $(j = 1, \ldots, n)$ ideais primos de S, distintos.*

b) *$\mathfrak{p}$ será totalmente inerte em L se, e somente se, $\overline{P}$ for irredutível em $\left(\frac{R}{\mathfrak{p}}\right)[x]$; neste caso, $\mathfrak{p} \cdot S$ é um ideal primo de S.*

c) *$\mathfrak{p}$ será totalmente ramificado em L se, e somente se, $\overline{P}$ for uma potência n-ésima em $\left(\frac{R}{\mathfrak{p}}\right)[x]$, isto é, $\overline{P} = (x - (a + \mathfrak{p}))^n$ para algum $a \in R$; neste caso $\mathfrak{p} \cdot S = \mathfrak{P}^n$, sendo $\mathfrak{P} = \mathfrak{p} \cdot S + (\beta - a) \cdot S$ um ideal primo de S.* ■

Diremos que o ideal primo não-nulo $\mathfrak{p}$ de R é *ramificado em L* quando existir um ideal primo $\mathfrak{P}$ de S acima de $\mathfrak{p}$ tal que $e(\mathfrak{P} \mid \mathfrak{p}) > 1$ ou que a extensão $\frac{S}{\mathfrak{P}}$ de $\frac{R}{\mathfrak{p}}$ seja inseparável.

Corolário A.52 *Com a hipótese e as notações do teorema A.50, as seguintes condições são equivalentes:*

(i) $\mathfrak{p}$ *é ramificado em* L.

(ii) *O polinômio* $\overline{p}_{\beta|K} \in \left(\frac{R}{\mathfrak{p}}\right)[x]$ *é inseparável.*

(iii) $disc(p_{\beta|K}) \in \mathfrak{p}$.

(iv) $\mathfrak{p}$ *divide* $\mathfrak{d}_{S|R}$.

Demonstração. Seja $P = p_{\beta|K}$. (i) $\iff$ (ii): Pelo teorema A.50, $\mathfrak{p}$ será ramificado em L se, e somente se, na fatoração $\overline{P} = \overline{P_1}^{e_1} \cdot \cdots \cdot \overline{P_r}^{e_r}$, tivermos que $e_j > 1$ ou $\overline{P}_j$ for inseparável para algum $j \in \{1, \ldots, r\}$; isto ocorrerá se, e somente se, $\overline{P}$ for inseparável.

(ii) $\iff$ (iii): Como $disc(P)$ é uma função simétrica nas raízes de P, existe $D \in \mathbb{Z}[x_1, \ldots, x_n]$ tal que $disc(P) = D(a_1, \ldots, a_n)$, onde,

$$P = x^n + a_1 x^{n-1} + \cdots + a_n;$$

portanto

$$disc(\overline{P}) = D(a_1 + \mathfrak{p}, \ldots, a_n + \mathfrak{p}) = D(a_1, \ldots, a_n) + \mathfrak{p}.$$

Concluimos que:

$$disc(P) \in \mathfrak{p} \iff disc(\overline{P}) = 0 \iff \overline{P} \text{ for inseparável.}$$

(iii) $\iff$ (iv): Segue do fato que $\mathfrak{d}_{S|R}$ é o ideal principal de R gerado por $disc_{L|K}(1, \beta, \ldots, \beta^{n-1}) = disc(P)$. ■

Referências Bibliográficas

[1] Borevich, Z. I., e Shafarevich, I. R., *Number Theory.* Academic Press, New York, 1966.

[2] Cohn, H. *Decomposition into four integral squares in the fields of* $2^{\frac{1}{2}}$ *and* $3^{\frac{1}{2}}$, Amer. J. Math. 82, 301-322 (1960).

[3] Deutsch, J. I. *Geometry of Numbers Proof of Götzky's Four-Squares Theorem.* Journal of Number Theory 96, 417-431 (2002).

[4] Endler, O. *Teoria dos Números Algébricos.* IMPA, Rio de Janeiro, 1985.

[5] Engler, A. J., e Brumatti, P., *Inteiros Quadráticos e o Grupo de Classes.* 23^o Colóquio Brasileiro de Matemática. IMPA, Rio de Janeiro, 2001.

[6] Garcia, A. L. e Lequain, Y., *Álgebra*: *Um Curso de Introdução.* IMPA, Rio de Janeiro, 1988.

[7] Gonçalves, A. *Introdução à Álgebra.* IMPA, Rio de Janeiro, 1979.

[8] Hardy, G. H., e Wright, E. M., *An Introduction to the Theory of Numbers*, quinta edição, Clarendon Press, Oxford, England, 1979.

[9] Hernstein, I. N. *Tópicos de álgebra.* Editôra da Univ. e Polígono, São Paulo, 1970.