Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Anel dos Inteiros Quadráticos

Por
Matheus Pereira Amorim

Sob orientação de
Josefa Itailma da Rocha

Campina Grande - PB
abril de 2022

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Matheus Pereira Amorim

Anel dos Inteiros Quadráticos

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em matemática.

Orientadora: Profª Drª Josefa Itailma da Rocha

Campina Grande - PB
abril de 2022

Dedicatória

Dedico esse trabalho a todos que me apoiaram durante minha trajetória pela matemática. Em especial, a minha família, professores e amigos. Sem a ajuda de cada um não seria possível eu estar aqui.

Agradecimento

Durante minha trajetória universitária, muitas pessoas foram fundamentais para meu sucesso. Independentemente do tamanho do papel e o quanto me ajudou, foram todos importantes.

Primeiramente, gostaria de agradecer aos meus pais, minha vó e minhas irmãs por me apoiarem na decisão de cursar matemática e em todas as minhas decisões acadêmicas. Gostaria de agradecer a meus amigos: Vitória, Vinícyus, Rayssa, Maysa, David, Brunna, Gustavo e Shara, por sempre estarem comigo desde o ensino médio e em todas as minhas crises.

Gostaria de agradecer ainda à Profª Drª Josefa Itailma da Rocha por orientar esse trabalho e me ajudar a concluir esse projeto durante os anos de estudo. E em tantos outros projetos que participei junto da professora, nos quais ela me orientou devo minha gratidão.

Gostaria de agradecer também a todos os professores que tive durante minha jornada acadêmica na UFCG. Principalmente, a todos os professores da UAMAT, que tiveram grande contribuição em estarem sempre dispostos a ensinar e ajudar no que fosse preciso.

Finalmente, gostaria de agradecer ao PET Matemática e Estatística. Os anos que passei no grupo me ajudaram muito a desenvolver como aluno e pessoa.

Resumo

Um elemento $\alpha = a+bi \in \mathbb{C}$ é dito um inteiro quadrático se α é um inteiro algébrico de $\mathbb{Q}[\sqrt{m}]$, ou equivalentemente, se $T(\alpha) = 2a$ e $N(\alpha) = \alpha\overline{\alpha}$ são números inteiros. Ao conjunto dos inteiros quadráticos chamamos de anel dos inteiros quadráticos e denotamos por $O(m)$. Este trabalho tem como objetivo estudar o anel $O(m)$, procurando caracterizar os seus elementos. Além disso, iremos estudar as unidades e ideais do anel $O(m)$, e para quais valores de m o anel é euclidiano. O estudo, em grande parte, será separado nos casos real ($m > 0$) e complexo ($m < 0$).

Palavras-chave: Inteiros; Quadráticos; Anel.

Abstract

An element $\alpha \in \mathbb{C}$ is a quadratic integer if α is an algebraic integer of $\mathbb{Q}[\sqrt{m}]$, or equivalently, if $T(\alpha) = 2a$ and $N(\alpha) = \alpha\overline{\alpha}$ are integer numbers. The set of quadratic integers is called ring of quadratic integers and we wil denotate $O(m)$. This paper has as an objective to study the ring $O(m)$, searching to characterize its elements. Besides that, we will study the units and ideals of the ring $O(m)$ and for which values of m the ring is euclidean. The study, on its majority, is divided on two cases: real ($m > 0$) and complex ($m < 0$).

Keywords: Integers; Quadratic; Ring.

Sumário

Introdução

A teoria dos números algébricos surgiu como uma ferramenta para a solução de problemas que envolvem números inteiros e soluções inteiras de equações conhecidas como Equações Diofantinas. Um exemplo desse tipo de problema é o famoso teorema enunciado pelo matemático francês Pierre de Fermat (1601 – 1665), conhecido como o Ultimo Teorema de Fermat, que afirma que não existem inteiros positivos x, y, z e n, com $n > 2$, tais que $x^n + y^n = z^n$.

Outro exemplo de grande importância nessa teoria são as chamada equações de Pell, que são equações da forma $x^2 - my^2 = 1$, com $m \in \mathbb{Z}$. As soluções dessas equações podem ser encontradas fazendo a fatoração $(x + d\sqrt{m})(x - d\sqrt{m}) = 1$. Como isso, observa-se a necessidade de considerar uma extensão dos números inteiros, e racionais, onde esteja inserido o $\sqrt{m}$. Tais extensões são conhecidas como corpos quadráticos $\mathbb{Q}[\sqrt{m}]$, onde m é um inteiro livre de quadrado.

Neste trabalho vamos estudar o anel $O(m)$ formados pelos inteiros algébricos do corpo quadrático $\mathbb{Q}[\sqrt{m}]$. Um elemento $\alpha \in \mathbb{C}$ é um inteiro algébrico se é raiz de um polinômico mônico com coeficientes em $\mathbb{Z}$. O conjunto $O(m)$ é um subanel de $\mathbb{Q}[\sqrt{m}]$ chamado de anel dos inteiros quadráticos. O objetivo principal desse trabalho é descrever o conjunto $O(m)$ dos inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$.

No Capítulo 1, caracterizaremos esses anéis através da sua norma e traço. Vamos também mostrar que os elemento de $O(m)$ são da forma $a + b\xi$, com $a, b \in \mathbb{Z}$ e

$$\xi = \begin{cases} \dfrac{1+\sqrt{m}}{2}, & \text{se } m \equiv 1 (mod\ 4) \\ \sqrt{m}, & \text{se } m \not\equiv 1 (mod\ 4) \end{cases}.$$

Assim, temos que $O(m) = \mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m}, \quad a, b \in \mathbb{Z}\}$, apenas quando $m \not\equiv 1 (mod\ 4)$.

No Capítulo 2, vamos estudar os anéis quadráticos euclidianos. Um anel domínio de integridade A é dito euclidiano se existe uma função $\varepsilon : A - \{0\} \longrightarrow \mathbb{N}$ tal que $\varepsilon(\alpha\beta) \geq \varepsilon(\alpha)$, para todo $\alpha, \beta \in A - \{0\}$ e existe um algoritmo da divisão em A, isto é, dados $\alpha, \beta \in A$, $\beta \neq 0$, existem $q, r \in A$ tais que $\alpha = q\beta + r$ com $r = 0$ ou $\varepsilon(r) < \varepsilon(\beta)$. No caso complexo, $O(m)$ é euclidiano para $m = -1, -2, -3, -7$ e -11 e são os únicos valores complexos para os quais isso acontece. No caso real, $O(m)$ é euclidiano para $m = 2, 3, 8, 6, 7, 11, 13, 17, 19, 21, 29,\ 33, 37, 41, 57$ e 73. No entanto, para o caso real, não garantimos que os valores escritos são os únicos, apenas conseguimos a finitude do conjuntos de tais valores. Este último fato foi provado em trabalhos de outros tais como H. Chatland [1], Barnes e Swinnerton-Dyer [2] e Samuel [3]. É bem conhecido que todo anel

euclidiano é um anel principal (ver Teorema 2.1.6). Na Seção 3.3 usaremos os anéis dos inteiros quadráticos para mostrar que a recíproca não é verdadeira. Mais especificamente, mostraremos que o anel $O(-19) = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ é um anel principal que não é euclidiano.

No Capítulo 3, estudaremos o conjunto $O(m)^*$, que é um subgrupo do grupo multiplicativo de $\mathbb{Q}[\sqrt{m}]$, chamado de grupo das unidades de $O(m)$. As unidades de $O(m)$ são os elementos $\mu \in O(m)$ tais que existe $\mu' \in O(m)$ com $\mu\mu' = 1$. No caso complexo, mostraremos que as unidades são

$$\pm 1, \pm\sqrt{-1}, \pm\xi \quad \text{e} \quad \pm\,\xi^2,$$

onde $\mu = \frac{1+\sqrt{m}}{2}$. No caso real, existe $\mu_0 \in O(m)^*$, chamado de unidade fundamental, tal que

$$O(m)^* = \{\pm\mu_0^n, n \in \mathbb{Z}\},$$

o que é um pouco mais complexo do que o caso real.

Finalmente, no Capítulo 4, iremos concluir nosso trabalho estudando os ideais de $O(m)$, mostrando que são representados na forma $(vk, v(u+\xi))$ onde $u, v, k > 0$ são inteiros. Ou seja, mostraremos que todo ideal I de $O(m)$ é da forma

$$I = \mathbb{Z} \oplus \mathbb{Z}v(u+\xi).$$

Capítulo 1

Anel dos Inteiros Quadráticos

Neste capítulo vamos introduzir os anéis dos inteiros quadráticos e caracterizar os seus elementos. Iniciaremos o estudo com os corpos quadráticos e os inteiros algébricos. O anel dos inteiros quadráticos, denota por $O(m)$, é formado pelos inteiros algébricos dos corpos quadráticos. Apresentaremos algumas propriedades dos inteiros algébricos e uma caracterização dos elementos de $O(m)$ que será usada nos próximos capítulos. Recomenda-se, para quem não está familiarizado com a teoria de números inteiros e anéis, a leitura de César e Sônia ([9], Capítulos 1, 2 e 3) e Vandernberg ([10], Parte III).

1.1 Corpos Quadráticos

Definição 1.1.1. *Um número complexo α é algébrico se existe um polinôimio não nulo $f(X) \in \mathbb{Q}[X]$ tal que $f(\alpha) = 0$, onde $\mathbb{Q}[X]$ é o anel dos polinômios sobre $\mathbb{Q}$.*

Exemplo 1.1.2. *Todo $\alpha \in \mathbb{Q}$ é algébrico, pois é raiz do polinômio*

$$P_\alpha(x) = x - \alpha \in \mathbb{Q}[X].$$

Exemplo 1.1.3. *Os números π e e (número de euler) são não algébricos. Estes números são chamados de transcendentes (veja [6, Capítulo 6, páginas 41-45] e [6, Capítulo 7, página 52]).*

Seja $\alpha \in \mathbb{C}$ algébrico, o polinômio mônico de menor grau em $\mathbb{Q}[X]$ que α anula é chamado de polinômio minimal de α. Como veremos a seguir, o polinômio minimal é único.

Proposição 1.1.4. *Seja $\alpha \in \mathbb{C}$ algébrico, então o polinômio minimal de α é único.*

Demonstração. Sejam $f(X)$ e $g(X)$ polinômios mônicos distintos em $\mathbb{Q}[X]$ e de mesmo e menor grau que anulam α, sendo assim o polinômio $(f-g)(X)$ é não nulo, anula α e tem grau menor que o de $f(X)$ e $g(X)$. Dividindo $(f-g)(X)$ pelo seu coeficiente do termo de maior grau, temos um polinômio mônico que anula α de grau menor que $f(X)$ e $g(X)$, contradizendo a minimalidade do grau dos mesmos. ∎

Definição 1.1.5. *Seja $\alpha \in \mathbb{C}$ algébrico, o conjunto $\mathbb{Q}[\alpha] = \{f(\alpha); f(X) \in \mathbb{Q}[X]\}$ é chamado de corpo algébrico. Dizemos que o corpo algébrico $\mathbb{Q}[\alpha]$ é um corpo quadrático se $\alpha \notin \mathbb{Q}$ e α anula um polinômio em $\mathbb{Q}[X]$ de grau 2.*

Exemplo 1.1.6. *Se m é um inteiro livre de quadrados, ou seja, m não é divisível por nenhum quadrado diferente de 1, então $\mathbb{Q}[\sqrt{m}]$ é um corpo quadrático. De fato, vejamos que:*

i) *Se m é um inteiro livre de quadrados, então $\sqrt{m} \notin \mathbb{Q}$: supondo que $\sqrt{m} \in \mathbb{Q}$, então existem inteiros p e q com $mdc(p,q) = 1$ tais que $\sqrt{m} = \frac{p}{q}$, daí*

$$m = \frac{p^2}{q^2} \Rightarrow p^2 = mq^2. \tag{1.1}$$

De (1.1), segue que $p|mq^2$. Como $mdc(p,q) = 1$, então $p|m$. Escreva $m = pp_1$, com $p_1 \in \mathbb{Z}$. Substituindo em (1.1), temos

$$p^2 = (pp_1)q^2 \Rightarrow p = p_1q^2 \tag{1.2}$$

Segue de (1.2) que $p|p_1$. Escrevendo $p_1 = pp_2$, temos

$$m = p(pp_2) = p^2p_2$$

donde $p^2|m$, o que é um absurdo pois m é um inteiro livre de quadrados. Logo, $\sqrt{m} \notin \mathbb{Q}$.

ii) *$\alpha = \sqrt{m}$ é raiz do polinômio*

$$p(X) = X^2 - m \in \mathbb{Q}[X]$$

Logo, $\mathbb{Q}[\sqrt{m}]$ é um corpo quadrático.

Proposição 1.1.7. *Todo corpo quadrático é da forma $\mathbb{Q}[\sqrt{m}]$, onde m é um inteiro livre de quadrados. Além disso, temos $\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m}; a, b \in \mathbb{Q}\}$.*

Demonstração. Seja $\mathbb{Q}[\alpha]$ um corpo quadrático. Como $\alpha \in \mathbb{Q}$ e é raiz de um polinômio em $\mathbb{Q}[X]$ de grau 2, então podemos escrever

$$\alpha = \frac{a + b\sqrt{m}}{c},$$

onde $a, b, c \in \mathbb{Q}$ e m é um inteiro livre de quadrados. Logo,

$$\mathbb{Q}[\alpha] = \mathbb{Q}\left[\frac{a + b\sqrt{m}}{c}\right] = \mathbb{Q}[\sqrt{m}].$$

e veremos a prova dessa igualdade mais a frente.

Vejamos que $\mathbb{Q}[\sqrt{m}] = \{a+b\sqrt{m}; a, b \in \mathbb{Q}\}$. Por definição, temos que $\mathbb{Q}[\sqrt{m}] = \{f(\sqrt{m}); f(X) \in \mathbb{Q}[X])\}$. Se $\alpha = a + b\sqrt{m}$, com $a, b \in \mathbb{Q}$, considerando $f(X) = a + bX \in \mathbb{Q}[X]$, temos que

$\alpha = f(\sqrt{m}) \in \mathbb{Q}[\sqrt{m}]$. Reciprocamente, seja $\alpha \in \mathbb{Q}[\sqrt{m}]$, então existe $f(X) \in \mathbb{Q}[X]$ tal que $\alpha = f(\sqrt{m})$. Sendo $p(X) = X^2 - m \in \mathbb{Q}[X]$, pelo algoritmo da divisão (ver [11, Teorema 23.1]) existem $q(X), r(X) \in \mathbb{Q}[X]$, com $r(X)$ nulo ou grau de $r(X)$ menor ou igual 1, tais que

$$f(X) = p(X)q(X) + r(X)$$

Daí sendo $r(X) = a + bX$, $a, b \in \mathbb{Q}$, e observando que $p(\sqrt{m}) = 0$, temos

$$\alpha = f(\sqrt{m}) = p(\sqrt{m})q(\sqrt{m}) + r(\sqrt{m}) = a + b\sqrt{m}.$$

Portanto, temos a igualdade

$$\mathbb{Q}\left[\frac{a + b\sqrt{m}}{c}\right] = \mathbb{Q}[\sqrt{m}].$$

■

As operações de soma e multiplicação em $\mathbb{Q}[\sqrt{m}]$ são definidas por: sendo $\alpha = a + b\sqrt{m}, \beta = c + d\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$, temos

$$\alpha + \beta = (a + c) + (b + d)\sqrt{m}$$
$$\alpha \cdot \beta = (ac + bdm) + (ad + bc)\sqrt{m}.$$

Além disso, se $\alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ e $\alpha \neq 0$, então

$$\alpha^{-1} = \frac{a}{a^2 - b^2m} - \frac{b}{a^2 - b^2m}\sqrt{m}. \tag{1.3}$$

Observa-se que $\mathbb{Q}[\sqrt{m}]$ é um subcorpo de $\mathbb{C}$.

Proposição 1.1.8. *Todo elemento de um corpo quadrático $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$ satisfaz um polinômio de grau 2 em $\mathbb{Z}[X]$*

Demonstração. Seja $\beta \in \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{m}]$, então $\beta = \dfrac{a + b\sqrt{m}}{c}$, onde $a, b, c \in \mathbb{Z}$, $mdc(a, b, c) = 1$ e m é livre de quadrados. Temos, $b\sqrt{m} = \beta c - a$ e assim $b^2m = \beta^2c^2 - 2ac\beta + a^2$ e portanto $\beta^2c^2 - 2ac\beta + a^2 - b^2m = 0$. Dessa última igualdade podemos concluir que β é raiz do polinômio $f(X) = c^2X - 2acX + a^2 - b^2m \in \mathbb{Z}[X]$. Portanto, todo elemento de $\mathbb{Q}[\alpha]$ satisfaz um polinômio de grau 2 em $\mathbb{Z}[X]$. ■

Observação 1.1.9. *Dados $a, b, c, d \in \mathbb{Q}$ e $a + b\sqrt{m} = c + d\sqrt{m} \Rightarrow a = c$ e $b = d$, ou seja, $\mathbb{Q}[\sqrt{m}]$ é determina de forma única seus elementos. Esse fato segue de $\sqrt{m} \notin \mathbb{Q}$.*

Dado um elemento $\alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ chamamos de conjugado de α, denotado por $\overline{\alpha}$, o elemento $\overline{\alpha} = a - b\sqrt{m}$. Definimos também o *traço* e *norma* de α por

$$T(\alpha) = \alpha + \overline{\alpha} = 2a \quad \text{e} \quad N(\alpha) = \alpha\overline{\alpha} = a^2 - mb^2$$

respectivamente. Observe que $T(\alpha)$ e $N(\alpha)$ pertecem a $\mathbb{Q}$.

No próximo resultado vamos mostrar algumas propriedades do traço e da norma que serão usadas ao longo do trabalho.

Proposição 1.1.10. *Dados $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$ temos:*

(a) $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$ *e* $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$.

(b) $\overline{\alpha} = \alpha$ *se, e somente se,* $\alpha \in \mathbb{Q}$.

(c) $T(\alpha + \beta) = T(\alpha) + T(\beta)$ *e* $N(\alpha\beta) = N(\alpha)N(\beta)$.

(d) $N(\alpha) = 0$ *se, e somente se,* $\alpha = 0$.

(e) *Se* $\alpha \neq 0$, *então* $\alpha^{-1} = \overline{\alpha}[N(\alpha)]^{-1}$.

(f) *Se* $m > 0$, *então* $|N(a + b\sqrt{m})| = |a^2 - mb^2| \leq max\{a^2, mb^2\}$.

Demonstração. Sejam $\alpha = a + b\sqrt{m}$ e $\beta = c + d\sqrt{m}$, então

$$\alpha + \beta = (a + c) + (b + d)\sqrt{m} \quad \text{e} \quad \alpha\beta = (ac + bdm) + (ad + bc)\sqrt{m}.$$

(a) Temos

$$\overline{\alpha} + \overline{\beta} = a - b\sqrt{m} + c - d\sqrt{m} = (a + c) - (b + d)\sqrt{m} = \overline{\alpha + \beta}$$
$$\overline{\alpha}\overline{\beta} = (a - b\sqrt{m})(c - d\sqrt{m}) = ac + bdm + (ad - bc)\sqrt{m} = \overline{\alpha\beta}$$

(b) É imediato que se $\alpha \in \mathbb{Q}$, então $\alpha = \overline{\alpha}$. Por outro lado, se $\overline{\alpha} = \alpha$ então $2b\sqrt{m} = 0$ o que implica em $b = 0$. Assim, $\alpha = a \in \mathbb{Q}$.

(c) Pelo item (a), temos:

$$T(\alpha + \beta) = \alpha + \beta + \overline{\alpha + \beta} = \alpha + \overline{\alpha} + \beta + \overline{\beta} = T(\alpha) + T(\beta)$$

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

(d) É imediato que se $\alpha = 0$, então $N(\alpha) = 0$. Se $N(\alpha) = 0$, então $\alpha\overline{\alpha} = 0$ o que implica em $\alpha = 0$ ou $\overline{\alpha} = 0$. Se o primeiro acontecer está provado; já se $\overline{\alpha} = 0$, então $a = b\sqrt{m}$, e assim $\alpha = 2a \in \mathbb{Q}$ e $\alpha = \overline{\alpha} = 0$.

(e) Primeiramente, observe que pelo item (c), com $\alpha \neq 0$, então $N(\alpha) \neq 0$ e assim existe $[N(\alpha)]^{-1} = (\alpha\overline{\alpha})^{-1} = (\overline{\alpha}^{-1})\alpha^{-1}$. Logo,

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

(f) Se $m > 0$, temos $-mb^2 \leq a^2 - mb^2 \leq a^2$. Logo, como sabemos que $N(a + b\sqrt{m}) = a^2 - mb^2$, então $|N(a + b\sqrt{m})| = |a^2 - mb^2|$. Daí, como consequência da desigualdade, $|a^2 - mb^2| \leq max\{a^2, mb^2\}$.

■

Proposição 1.1.11. *Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$. Então α é raíz do polinômio.*

$$f_\alpha(x) = x^2 - T(\alpha)x + N(\alpha) \in \mathbb{Q}[X].$$

Demonstração. Seja $\alpha = a + b\sqrt{m}$, então:

$$\alpha^2 = (a + b\sqrt{m})(a + b\sqrt{m}) = a^2 + 2ab\sqrt{m} + b^2m.$$

Assim,

$$\begin{aligned} f_\alpha(\alpha) &= a^2 + 2ab\sqrt{m} + b^2m - 2a(a + b\sqrt{m}) + a^2 - b^2m \\ &= 2a^2 + 2ab\sqrt{m} - 2a^2 - 2ab\sqrt{m} = 0. \end{aligned}$$

■

1.2 Inteiros Quadráticos

Definição 1.2.1. *Seja $\alpha \in \mathbb{C}$. Dizemos que α é um inteiro algébrico se α anula um polinômio mônico $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. Nestas condições, chamamos α de inteiro ou integral sobre $\mathbb{Z}$. Definimos então os inteiros de $\mathbb{Q}[\sqrt{m}]$ como sendo o conjunto dos inteiros algébricos que estão em $\mathbb{Q}[\sqrt{m}]$. Denotaremos por $O(m)$.*

Exemplo 1.2.2. *Todo inteiro é um inteiro algébrico. De fato, seja $\alpha \in \mathbb{Z}$, note que α é raiz do seguinte polinômio*

$$f(X) = X - \alpha \in \mathbb{Z}[X].$$

Logo α é um inteiro algébrico.

Exemplo 1.2.3. *$\sqrt{m}$ é um inteiro algébrico. De fato, $\sqrt{m}$ é raiz de*

$$g(X) = X^2 - m \in \mathbb{Z}[X].$$

Observação 1.2.4. *Por [7, Corolário 1.3] o conjunto $O(m)$ dos inteiros de $\mathbb{Q}[\sqrt{m}]$ é um anel. Mais precisamente, é um subanel de $\mathbb{Q}[\sqrt{m}]$.*

Podemos caracterizar os elementos de $O(m)$ através do traço e da norma. Para isso, vamos precisar dos seguintes resultados:

Observação 1.2.5. *Se $\alpha \in O(m)$, então $\overline{\alpha} \in O(m)$. De fato, seja $\alpha = a + b\sqrt{m} \in O(m)$ e considere $p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ o polinômio mônico que anula α, ou seja, $p(\alpha) = 0$. Vamos verificar $\overline{\alpha}$ também é raiz de $p(X)$. Primeiramente, observe que*

$$0 = p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 \tag{1.4}$$

Assim, aplicando o conjugado em (1.4)

$$0 = \overline{\alpha}^n + a_{n-1}\overline{\alpha}^{n-1} + \cdots + a_0 = p(\overline{\alpha})$$

Portanto, $\overline{\alpha} \in O(m)$.

Lema 1.2.6. *Seja $\alpha \in \mathbb{Q}$ tal que existe um polinômio mônico $g(x) \in \mathbb{Z}[X]$, satisfazendo $g(\alpha) = 0$. Então $\alpha \in \mathbb{Z}$.*

Demonstração. Seja $\alpha = \dfrac{a}{b}$ com $b \geq 1$ (a e b primos entre si) e $g(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + X^n$ com $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$. Então

$$0 = g(\alpha) = a_0 + a_1\frac{a}{b} + a_2\frac{a^2}{b^2} + \cdots + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \frac{a^n}{b^n}$$

Multiplicando ambos os lado por b^n, temos

$$\begin{aligned} 0 &= b^n g(\alpha) = b^n a_0 + b^{n-1}a_1 a + b^{n-2}a_2 a^2 + \cdots + b a_{n-1}a^{n-1} + a^n \\ &= b(b^{n-1}a_0 + b^{n-2}a_1 a + b^{n-3}a_2 a^2 + \cdots + a_{n-1}a^{n-1}) + a^n. \end{aligned}$$

Segue da ultima igualdade que b divide a^n. Consequentemente, como $mdc(a, b) = 1$, devemos ter $b = 1$. Logo, $\alpha = a \in \mathbb{Z}$.

■

Teorema 1.2.7. *Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$. Então $\alpha \in O(m)$ se, e somente se, $T(\alpha)$ e $N(\alpha)$ são inteiros.*

Demonstração. Suponha que $N(\alpha), T(\alpha) \in \mathbb{Z}$. Então, pela Proposição 1.1.11, temos que α é raiz do polinômio mônico

$$f(X) = X^2 - T(\alpha)X + N(\alpha) \in \mathbb{Z}[X].$$

Logo, α é um inteiro quadrático e portanto $\alpha \in O(m)$.

Reciprocamente, seja $\alpha \in O(m)$. Pela Observação 1.2.5 temos que $\overline{\alpha} \in O(m)$. Além disso, como $O(m)$ é um anel, segue que

$$T(\alpha) = \alpha + \overline{\alpha}, \quad N(\alpha) = \alpha\overline{\alpha} \in O(m).$$

Logo, existem polinômios mônicos $f(X), g(X) \in \mathbb{Z}[X]$ tais que

$$f(T(\alpha)) = 0 \quad \text{e} \quad g(N(\alpha)) = 0.$$

Portanto, pelo Lema 1.2.6, temos que $T(\alpha)$ e $N(\alpha)$ são inteiros.

■

Corolário 1.2.8. *Todo inteiro de $\mathbb{Q}[\sqrt{m}]$ anula um polinômio mônico de grau 2 em $\mathbb{Z}[X]$.*

Demonstração. É imediato pelo Teorema 1.2.7 e pela Proposição 1.1.11. ■

Com essa caracterização podemos mostrar as seguintes propriedades de $O(m)$.

Corolário 1.2.9. $\mathbb{Z} = O(m) \cap \mathbb{Q}$.

Demonstração. É imediato pelo Lema 1.2.6 e pelo fato de que todo inteiro pertence a $O(m)$. ■

Observação 1.2.10. *Seja $\alpha = a + b\sqrt{m}$, com $a, b \in \mathbb{Z}$, então $T(\alpha) = 2a$ e $N(\alpha) = a^2 - mb^2$ são inteiros e, pelo Teorema 1.2.7, temos que $\alpha \in O(m)$. Assim, vale a inclusão $\mathbb{Z}[\sqrt{m}] \subseteq O(m)$. Porém, a inclusão contrária nem sempre é verdadeira. De fato, para $m = -3$, considere $\xi = \frac{-1+\sqrt{-3}}{2} \in \mathbb{Q}[\sqrt{-3}]$. Temos*

$$T(\xi) = 2.\left(\frac{-1}{2}\right) = -1 \quad e \quad N(\xi) = \left(\frac{-1}{2}\right)^2 - 3\left(\frac{1}{2}\right)^2 = 1.$$

Assim, $T(\xi), N(\xi) \in \mathbb{Z}$ e portanto $\xi \in O(-3)$. Porém, $\xi \notin \mathbb{Z}[\sqrt{-3}]$.

No próximo resultado apresentaremos uma caracterização dos elementos de $O(m)$ e veremos que a igualdade $O(m) = \mathbb{Z}[\sqrt{m}]$ só é válida se $m \not\equiv 1(mod\ 4)$.

Teorema 1.2.11. *Sejam m um inteiro livre de quadrados e $\alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$. Temos então dois casos a considerar:*

(a) *Se $m \equiv 1(mod\ 4)$, então $\alpha \in O(m)$ se, e somente se, $2a, 2b \in \mathbb{Z}$ e ambos tem mesma paridade.*

(b) *Se $m \not\equiv 1(mod\ 4)$, então $\alpha \in O(m)$ se, e somente se, $a, b \in \mathbb{Z}$.*

Demonstração.

(a) ($\Rightarrow$) Se $\alpha \in O(m)$, então $T(\alpha) = 2a \in \mathbb{Z}$ e $4N(\alpha) = (2a)^2 - m(2b)^2 \in \mathbb{Z}$. Como $2a$ é inteiro, logo $m(2b)^2 = 4N(\alpha) - (2a)^2 \in \mathbb{Z}$, pois é a diferença de dois inteiros. Suponha que $2b \notin \mathbb{Z}$, então $2b = p/q$, com $p, q \in \mathbb{Z}$, $q > 1$ e $mdc(p, q) = 1$. Assim,

$$m(2b)^2 = m\frac{p^2}{q^2} \in \mathbb{Z}$$

donde segue que q^2 divide mp^2. Como $mdc(p, q) = 1$, então q^2 deve dividir m, o que é um absurdo, já que m é livre de quadrados. Logo, $2b \in \mathbb{Z}$. Por fim, como 4 divide $(2a)^2 - m(2b)^2$ e 4 não divide m, segue que $2a$ é par se, e somente se , $2b$ é par.

($\Leftarrow$) Vamos verificar agora que se $m \equiv 1(mod\ 4)$ e $a, b \in \mathbb{Q}$ são tais que $2a, 2b \in \mathbb{Z}$ e tem mesma paridade, então $\alpha \in O(m)$. Inicialmente $T(\alpha) = 2a \in \mathbb{Z}$. Resta mostrar que $N(\alpha) \in \mathbb{Z}$. Observe que

$$N(\alpha) = a^2 - mb^2 = \frac{|(2a)^2 - m(2b)^2|}{4}.$$

Como $2a$ e $2b$ tem mesma paridade, então $(2a)^2 \equiv (2b)^2(mod\ 4)$. Por outro lado, por $m \equiv 1(mod\ 4)$, então $m(2b)^2 \equiv (2a)^2(mod\ 4)$. Logo,

$$(2a)^2 - m(2b)^2 \equiv 0(mod\ 4)$$

ou seja, 4 divide $(2a)^2 - m(2b)^2$ e portanto $N(\alpha) \in \mathbb{Z}$.

(b) ($\Leftarrow$) Se $a, b \in \mathbb{Z}$, então $\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}] \subseteq O(m)$.

($\Rightarrow$) Seja $\alpha = a + b\sqrt{m} \in O(m)$ e suponha que $a \notin \mathbb{Z}$. Como $T(\alpha) = 2a \in \mathbb{Z}$ então $2a$ é um inteiro ímpar. Por $N(\alpha) \in \mathbb{Z}$, temos que

$$4N(\alpha) = (2a)^2 - m(2b)^2 \in 4\mathbb{Z}$$

e assim $2b$ deve ser ímpar também. Logo, de $(2a)^2 \equiv (2b)^2 (mod\ 4)$ e $(2a)^2 \equiv m(2b)^2 (mod\ 4)$. Como b ímpar, temos $mdc(4, (2b)^2) = 1$ e devemos ter $m \equiv 1 (mod\ 4)$, o que é um absurdo. Daí, $a \in \mathbb{Z}$. O caso em que $b \notin \mathbb{Z}$ é análogo.

■

Concluímos pela demonstração do Teorema 1.2.11 que

$$O(m) = \left\{ \frac{a + b\sqrt{m}}{2} \quad | \quad a, b \in \mathbb{Z} \quad \text{e} \quad a \equiv b (mod\ 2) \right\}$$

se $m \equiv 1 (mod\ 4)$, e que

$$O(m) = \{a + b\sqrt{m};\ a, b \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{m}],$$

se $m \not\equiv 1 (mod\ 4)$. Portanto, a inclusão da Observação 1.2.10 é própria se, e somente se, $m \equiv 1 (mod\ 4)$.

No próximo resultado apresentaremos outra maneira de escrever os elementos de $O(m)$, quando $m \equiv 1 (mod\ 4)$, que será usada nos próximos capítulos.

Teorema 1.2.12. *Se $m \equiv 1 (mod\ 4)$, então* $O(m) = \left\{ a + b\xi \quad | \quad a, b \in \mathbb{Z} \quad e \quad \xi = \frac{1 + \sqrt{m}}{2} \right\}$.

Demonstração. Basta provarmos que $\alpha \in O(m)$ se, e somente se, existem a e $b \in \mathbb{Z}$ tais que $\alpha = a + b\xi$. Se $\alpha = c + d\sqrt{m} \in O(m)$, então $2c, 2d \in \mathbb{Z}$ e têm mesma paridade. Logo $c + d = (2c + 2d)/2 \in \mathbb{Z}$. Considerando $a = c - d$ e $b = 2d$, temos que

$$a + b\xi = c - d + 2d\left(\frac{1 + \sqrt{m}}{2}\right) = c - d + d + d\sqrt{m} = c + d\sqrt{m} = \alpha.$$

Reciprocamente, dado $\alpha = a + b\xi$, com $a, b \in \mathbb{Z}$, temos

$$\alpha = a + b\left(\frac{1 + \sqrt{m}}{2}\right) = a + \frac{b}{2} + \frac{b}{2}\sqrt{m} = \left(\frac{2a + b}{2}\right) + \frac{b}{2}\sqrt{m}$$

Sendo a e b inteiros, temos que

$$2\left(\frac{2a + b}{2}\right) = 2a + b \in \mathbb{Z} \quad \text{e} \quad 2\frac{b}{2} = b \in \mathbb{Z}.$$

Além disso, como $2a$ é par, então $2a + b$ e b têm mesma paridade. Portanto, pelo Teorema 1.2.11, temos que $\alpha \in O(m)$.

■

Pelos Teoremas 1.2.11 e 1.2.12, concluímos que $O(m) = \mathbb{Z}[\xi] = \{a + b\xi; a, b \in \mathbb{Z}\}$ onde

$$\xi = \begin{cases} \dfrac{1+\sqrt{m}}{2}, & \text{se } m \equiv 1(mod\ 4) \\ \sqrt{m}, & \text{se } m \not\equiv 1(mod\ 4) \end{cases}.$$

Chamaremos os anéis quadráticos $O(m)$ com $m < 0$ de *anéis quadráticos complexos* e, para $m > 0$, chamaremos de *anéis quadráticos reais.* Por exemplo, se $m = 6 \equiv 2(mod\ 4)$, o anel

$$O(6) = \mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6};\ a, b \in \mathbb{Z}\}$$

é um anel quadrático real. Para $m = -3 \equiv 1(mod\ 4)$, o anel

$$O(-3) = \left\{a + b\left(\frac{1+\sqrt{-3}}{2}\right);\ a, b \in \mathbb{Z}\right\}$$

é um anel quadrático complexo.

Capítulo 2

Anéis Quadráticos Euclidianos

Neste Capítulo vamos estudar os anéis quadráticos euclidianos. Um anel é dito Euclidiano quando possui um algoritmo de divisão. Veremos que existem apenas 28 valores de m para os quais o anel $O(m)$ é euclidiano. O estudo será divido no caso real e imaginário. No caso real, as demonstrações são bastante complexas e podem ser encontradas em [1], [2] e [3], e por isso faremos apenas as demonstrações de alguns resultados parciais. Apresentaremos alguns exemplos de como funciona o algoritmo da divisão nesses anéis. Usaremos também os anéis dos inteiros quadrático para fornecer um exemplo de um anel principal que não é euclidiano, exemplo clássico da Teoria de Anéis.

2.1 Anéis Euclidianos

Definição 2.1.1. *Um domínio A é um anel euclidiano se existe uma aplicação $\varepsilon : A - \{0\} \to \mathbb{Z}^+$ tal que:*

1. *$\varepsilon(\alpha\beta) \geq \varepsilon(\alpha)$, para todo $\alpha, \beta \in A - \{0\}$.*
2. *Existe um algoritmo da divisão em A, isto é, dados $\alpha, \beta \in A$, $\beta \neq 0$, existem $q, r \in A$ tais que $\alpha = q\beta + r$ com $r = 0$ ou $\varepsilon(r) < \varepsilon(\beta)$.*

Observação 2.1.2. *Note que na definição anterior não exigirmos a unicidade de q e r no algoritmo da divisão.*

Observação 2.1.3. *Chamaremos a função ε de norma euclidiana ou valorização euclidiana.*

Exemplo 2.1.4. *O anel dos inteiros $\mathbb{Z}$ atribuindo-se a norma, isto é, dado $n \in \mathbb{Z}$ temos que a aplicação $n \mapsto |n|$ satisfaz a definição para que $\mathbb{Z}$ seja euclidiano.*

Exemplo 2.1.5. *Se A é um corpo, então o anel dos polinômios $A[X]$ é um anel euclidiano, onde a função ε é dada pelo grau do polinômio, ou seja, dados $f(X), g(X) \in A[X]$, com $g(X) \neq 0$,*

existem $q(X), r(X) \in A[X]$ *tais que*

$$f(X) = q(X)g(X) + r(X),$$

onde $r(X) = 0$ *ou* $\partial(r(x)) < \partial(g(X))$ *(ver [11, Teorema 23.1]).*

Seja A um domínio e $a \in A$. O conjunto

$$< a >= \{ax;\ x \in A\}$$

é um ideal de A, chamado de *ideal principal gerado por* a. É fácil ver que $< a >$ é o menor ideal de A que contém a, ou seja, se I é um ideal de A e $a \in I$, então $< a > \subseteq I$. Um domínio A é chamado de *anel principal* quando todo ideal I de A é principal, isto é, para cada ideal I existe $a \in A$ tal que $I =< a >$.

Dados $\alpha, \beta \in O(m) - \{0\}$ dizemos que α divide β em $O(m)$, e denotamos $\alpha \mid \beta$, se existe $\gamma \in O(m)$ tal que $\beta = \alpha\gamma$. Assim, temos que α divide β se, e somente se, $\beta \in < \alpha >$.

O próximo resultado relaciona os anéis euclidianos com os anéis principais.

Teorema 2.1.6. *Todo anel euclidiano é um anel principal.*

Demonstração. Seja A um anel euclidiano e ε uma valorização euclidiana de A. Consideremos I um ideal de A, com $I \neq \{0\}$, e tomemos $b \in I - \{0\}$ tal que $\varepsilon(b) = min\{\varepsilon(x) | x \in I - \{0\}\}$. Mostremos que $I =< b >$. De fato, como $b \in I$, então $< b > \subseteq I$. Tomando agora $a \in I$, como $b \neq 0$, devem existir q, $r \in A$, com $r = 0$ ou $\varepsilon(r) < \varepsilon(b)$, tais que $a = bq + r$. Como $a, bq \in I$, concluímos que $r \in I$ e portanto $r = 0$, pois se $r \neq 0$ então $\varepsilon(r) < \varepsilon(b)$, o que seria uma contradição. Assim, $a = bq \in < b >$ e portanto $I =< b >$.

■

Observação 2.1.7. *A recíproca do Teorema 2.1.6 não é sempre válida. Na Seção 2.3 vamos usar os anéis dos inteiros quadráticos para apresentar um exemplo de um anel principal que não é euclidiano.*

2.2 Anéis Quadráticos Euclidianos

Agora, tendo em vista o que estudamos, vamos usar a função norma N, mais precisamente o módulo da norma $|N|$, como norma euclidiana em $O(m)$ (anel dos inteiros quadráticos). Vale observar que a primeira condição da norma euclidiana é sempre satisfeita para o módulo da norma, isto é,

$$|N(\alpha\beta)| \geq |N(\alpha)| \text{ para todo } \alpha, \beta \in O(m) - \{0\}.$$

De fato, da Proposição 1.1.10 $|N(\alpha\beta)| = |N(\alpha)N(\beta)|$, pelo Teorema 1.2.7 $N(\alpha), N(\beta) \in \mathbb{Z}$, daí $|N(\alpha)N(\beta)| = |N(\alpha)||N(\beta)|$. Pelo estudo dos inteiros,

$$|N(\alpha)||N(\beta)| \geq |N(\alpha)|$$

obtendo o que queríamos.

Para a segunda condição da norma euclidiana vamos usar o seguinte resultado:

Lema 2.2.1. *A função $\varepsilon(\alpha) = |N(\alpha)|$ é uma norma euclidiana para $O(m)$ se, e somente se, dado $\gamma \in \mathbb{Q}[\sqrt{m}]$, existe $\delta \in O(m)$ tal que $|N(\gamma - \delta)| < 1$.*

Demonstração. ($\Rightarrow$) Suponha que $\varepsilon(\alpha) = |N(\alpha)|$ é uma norma euclidiana para $O(m)$. Seja $\gamma \in \mathbb{Q}[\sqrt{m}]$. Se $\gamma \in O(m)$, considerando $\delta = \gamma \in O(m)$, temos

$$|N(\gamma - \delta)| = |N(0)| = 0 < 1$$

e a condição é satisfeita. Suponha $\gamma \notin O(m)$, então $\gamma = \dfrac{\alpha}{\beta}$, com $\alpha, \beta \in O(m)$, e assim podemos escrever $\beta = \alpha\gamma^{-1} \in O(m)$. Como $O(m)$ é euclidiano, existem $\delta, r \in O(m)$ tais que

$$\alpha = \beta\delta + r \quad \text{e} \quad |N(r)| < |N(\beta)|.$$

Escrevendo $r = \alpha - \beta\delta$, temos $|N(\alpha - \beta\delta)| < |N(\beta)|$. Por outro lado, pela Proposição 1.1.10 item (c), temos

$$|N(\alpha - \beta\delta)| = |N(\beta(\alpha\beta^{-1} - \delta))| = |N(\beta)||N(\alpha\beta^{-1} - \delta)| < |N(\beta)|,$$

o que implica que $|N(\alpha\beta^{-1} - \delta)| < 1$, ou equivalentemente $|N(\gamma - \delta)| < 1$.

($\Leftarrow$) Dados $\beta, \alpha \in O(m)$, $\beta \neq 0$, seja $\gamma = \alpha\beta^{-1}$. Por hipótese, existe $\delta \in O(m)$ tal que $|N(\gamma - \delta)| < 1$. Observe que

$$\alpha = \beta\delta + (\alpha - \beta\delta)$$

e

$$\begin{aligned} |N(\alpha - \beta\delta)| &= |N(\beta(\alpha\beta^{-1} - \delta))| = |N(\beta)||N(\alpha\beta^{-1} - \delta)| \\ &= |N(\beta)||N(\gamma - \delta)| < |N(\beta)|. \end{aligned}$$

Portanto, $O(m)$ é um anel euclidiano com $\varepsilon(\alpha) = |N(\alpha)|$.

■

Observação 2.2.2. *Pela demonstração do Lema 2.2.1 segue que se $O(m)$ é um anel euclidiano, então o quociente da divisão de α por β é dado por $\delta \in O(m)$ que satisfaz*

$$\left| N\left(\frac{\alpha}{\beta} - \delta\right) \right| < 1.$$

Utilizando o Lema 2.2.1 exibiremos uma lista de valores de m para os quais $O(m)$ tem norma euclidiana.

Teorema 2.2.3. *A função $|N|$ é uma norma euclidiana para $O(m)$ nos casos em que $m = -11, -7, -3, -2, -1, 2, 3, 5, 13$.*

Demonstração. Considere $m = -2, -1, 2, 3$, neste caso temos $m \not\equiv 1(mod\ 4)$ e assim $O(m) = \mathbb{Z}[\sqrt{m}]$. Dado $\gamma = u + v\sqrt{m}$, com $u, v \in \mathbb{Q}$, tome $s, t \in \mathbb{Z}$ tais que $|u - s| \leq 1/2$ e $|v - t| \leq 1/2$. Para $\delta = s + t\sqrt{m} \in O(m)$ tem-se que $\gamma - \delta = (u - s) + (v - t)\sqrt{m}$. Logo

$$|N(\gamma - \delta)| = |(u - s)^2 - m(v - t)^2| \leq (u - s)^2 + |m|(v - t)^2 \leq \frac{1 + |m|}{4} < 1$$

se $m = -2, -1$, ou 2. Se $m = 3$ temos que na primeira desigualdade acima só ocorre igualdade se $u = s$ ou $v = t$ e nesse caso a expressão tem valor menor que 1. Se $u \neq s$ e $v \neq t$ a primeira desigualdade é estrita e assim a expressão tem valor menor que 1. Logo $|N(\gamma - \delta)| < 1$ em todos os casos.

Para $m = -11, -7, -3, 5$ e 13, temos $m \equiv 1(mod\ 4)$ e assim

$$O(m) = \left\{ \frac{a + b\sqrt{m}}{2}; a, b \in \mathbb{Z} \ \text{ e } \ a \equiv b(mod\ 2) \right\}.$$

Seja $\gamma = u + v\sqrt{m}$, com $u, v \in \mathbb{Q}$ e considere $t, s \in \mathbb{Z}$ de mesma paridade tais que $|t/2 - v| \leq 1/4$ e $|s/2 - u| \leq 1/2$. Tome $\delta = \dfrac{s + t\sqrt{m}}{2} \in O(m)$, então se $m < 0$, temos

$$|N(\gamma - \delta)| = |(u - s/2)^2 - m(v - t/2)^2| \leq |u - s/2|^2 + |m||v - t/2|^2 \leq \frac{1}{4} + \frac{|m|}{16} < 1$$

para $m = -11, -7, -3$.

Se $m > 0$, segue da Proposição 1.1.10 que

$$|N(\gamma - \delta)| = |(u - s/2)^2 - m(v - t/2)^2| \leq \text{máx} \left\{ \frac{1}{4}, \frac{m}{16} \right\} < 1$$

para $m = 5, 13$.

■

A seguir vamos apresentar alguns exemplos para mostrar como o algoritmo da divisão funciona nos anéis euclidianos $O(m)$. Para isso, vamos usar a Observação 2.2.2 e a demonstração do Teorema 2.2.3.

Exemplo 2.2.4. *Sejam $m = 2 \equiv 2(mod\ 4)$ e $\alpha = 12 + 3\sqrt{2}, \beta = 5 \in O(2)$. Queremos encontrar $q = s + t\sqrt{2}, r = x + y\sqrt{2} \in O(2)$, tais que $\alpha = \beta q + r$ e $|N(r)| < |N(\beta)|$. Pela Observação 2.2.2, temos que q satisfaz a condição*

$$\left| N\left(\frac{\alpha}{\beta} - q \right) \right| < 1.$$

Escreva $\dfrac{\alpha}{\beta} = \dfrac{12}{5} + \dfrac{3}{5}\sqrt{2} = u + v\sqrt{2}$. Pela demonstração do Teorema 2.2.3, vamos tomar $t, s \in \mathbb{Z}$ tais que $|u - s| < 1/2$ e $|v - t| < 1/2$. Considerando então $s = 2$ e $t = 1$, temos

$$\left|\frac{12}{5}-2\right| = \left|\frac{2}{5}\right| < \frac{1}{2} \quad e \quad \left|\frac{3}{5}-1\right| = \left|\frac{-2}{5}\right| < \frac{1}{2}.$$

Assim, podemos considerar $q = 2+\sqrt{2}$. *Para determinar* r *vamos usar a relação* $r = \alpha - q\beta$, *assim*

$$r = 12 + 3\sqrt{2} - (2+\sqrt{2})\cdot 5 = 2 - 2\sqrt{2}.$$

Temos portanto que

$$12 + 3\sqrt{2} = 5\cdot(2+\sqrt{2}) + (2-2\sqrt{2}),$$

onde

$$|N(2-2\sqrt{2})| = |2^2 - 2\cdot(-2)^2| = 4 < 25 = |N(5)|.$$

Exemplo 2.2.5. *Sejam* $m = -11 \equiv 1(mod\ 4)$, $\alpha = 19 + 10\sqrt{-11}$ *e* $\beta = 6$. *Vamos encontrar* $q = x + y\sqrt{-11}, r \in O(-11) = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$, *tais que* $\alpha = q\beta + r$ *com* $|N(r)| < |N(6)|$. *Escreva*

$$\frac{\alpha}{\beta} = u + v\sqrt{-11} = \frac{19}{6} + \frac{10}{6}\sqrt{-11}.$$

Seguindo a demonstração do Teorema 2.2.3, vamos tomar inicialmente $y = \frac{t}{2}$ *com* $t \in \mathbb{Z}$ *tal que* $|v-y| \leq \frac{1}{4}$. *Considere* $y = \frac{3}{2}$. *Então,*

$$|v-y| = \left|\frac{5}{3} - \frac{3}{2}\right| = \frac{1}{6} \leq \frac{1}{4}$$

Vamos tomar agora $x = \frac{s}{2}$ *com* $s \in \mathbb{Z}$ *número ímpar tal que* $|u-x| \leq \frac{1}{2}$. *Considere* $x = \frac{7}{2}$. *Assim,*

$$|u-x| = \left|\frac{19}{6} - \frac{7}{2}\right| = \left|\frac{-2}{6}\right| = \frac{1}{3} \leq \frac{1}{2}$$

Pela Observação 2.2.2, temos

$$q = \frac{7}{2} + \frac{3}{2}\sqrt{-11} \quad e \quad r = \alpha - q\beta = -2 + \sqrt{-11}$$

onde

$$|N(r)| = |4+11| = 15 < 36 = |N(6)|.$$

2.2.1 Anéis Quadráticos Euclidianos Complexos

No Teorema 2.2.3, obtemos que $|N|$ é uma norma euclidiana para $O(m)$ quando $m = -1, -2, -3, -7$ e -11. Vamos mostrar a seguir que esses são os únicos valores negativos de m para os quais isso ocorre em relação à norma $|N|$.

Teorema 2.2.6. *Se $m < 0$ e $O(m)$ é euclidiano em relação a $|N|$, então $m = -1, -2, -3, -7$ ou -11.*

Demonstração. Se $O(m)$ é euclidiano, conforme Lema 2.2.1, para cada $0 \neq \alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$, existe $\beta \in O(m)$,

$$\beta = \begin{cases} r + s\sqrt{m}, \ r, s \in \mathbb{Z}, & \text{se } m \not\equiv 1(mod\ 4) \\ \dfrac{r + s\sqrt{m}}{2}, \ r, s \in \mathbb{Z} \ \ e \ \ r \equiv s(mod\ 2), & \text{se } m \equiv 1(mod\ 4) \end{cases}$$

tal que $|N(\alpha - \beta)| < 1$. Explicitando o valor da norma temos

$$|(a-r)^2 - m(b-s)^2| < 1, \quad \text{se} \ \ m \not\equiv 1(mod\ 4) \tag{2.1}$$

$$|(a - r/2)^2 - m(b - s/2)^2| < 1 \ \ \text{se} \ \ m \equiv 1(mod\ 4) \tag{2.2}$$

Consideremos primeiro o caso $m \not\equiv 1(mod\ 4)$. Fazendo $a = 1/2$ e $b = 1/2$, reescrevemos (2.1) da seguinte forma

$$|(1 + |m|)/4 + [(r^2 - r) + |m|(s^2 - s)]| < 1. \tag{2.3}$$

Como para todo inteiro x vale $x^2 - x \geq 0$, temos que $[(r^2 - r) + |m|(s^2 - s)] \geq 0$. Combinando a última desigualdade com a (2.3) obtemos $(1 + |m|)/4 < 1$, o que implica em $|m| < 3$, isto é, $m = -1$ ou $m = -2$.

No caso $m \equiv 1(mod\ 4)$ tomamos $a = 1/4$ e $b = 1/4$ em (2.2):

$$|(1 + |m|)/16 + [(r^2/4 - r/4) + |m|(s^2/4 - s/4)]| < 1$$

Novamente, por $(1/4)[(r^2 - r) + |m|(s^2 - s)] \geq 0$ devemos ter $(1 + |m|)/16 < 1$. Dessa forma $|m| < 15$ e como $m \equiv 1(mod\ 4)$, obtemos $m = -3, -7$ e -11.

■

Pelos Teoremas 2.2.3 e 2.2.6 temos que se $m < 0$, então $|N|$ é uma norma euclidiana para $O(m)$ se, e somente se, $m = -1, -2, -3, -7$ e -11. Segundo Samuel ([3], Proposição 14), para $m < 0$, $O(m)$ é euclidiano para alguma norma euclidiana ε se, e somente se, é euclidiano para $|N|$. Consequentemente, temos que esses são os únicos valores de $m < 0$ para os quais $O(m)$ é euclidiano para alguma norma euclidiana.

2.2.2 Anéis Quadráticos Euclidianos Reais

Pelo Teorema 2.2.3 temos que $O(m)$ é euclidiano para $m = 2, 3, 5$ e 13. Em geral, $O(m)$ é euclidiano com a norma $|N|$ apenas para $m = 2, 3, 8, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57$ e 73. Esse resultado foi provado em uma série de trabalhos tais como H. Chatland [1], Barnes e Swinnerton-Dyer [2] e Samuel [3].

As demonstrações desses resultados são bastante complicadas. Nessa seção, vamos apresentar alguns resultados parciais. No próximo resultado apresentaremos a demonstração de que $O(m)$ é euclidiano para $m = 6, 7, 17, 21$ e 29.

Teorema 2.2.7. *A função $|N|$ é uma norma euclidiana para $O(m)$ nos casos $m = 6, 7, 17, 21$ e 29.*

Demonstração. Como no Teorema 2.2.3, basta mostrar que dado $\gamma = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ existe $\delta \in O(m)$ tal que $|N(\gamma - \delta)| < 1$. Observe que se $m \equiv 2, 3 (mod\ 4)$, então $\delta = x + y\sqrt{m}$, com $x, y \in \mathbb{Z}$, e assim queremos

$$|N(\gamma - \delta)| = |(a - x)^2 - m(b - y)^2| < 1. \tag{2.4}$$

Sendo $x_0, y_0 \in \mathbb{Z}$ tais que $|a - x_0| \leq \frac{1}{2}$ e $|b - y_0| \leq \frac{1}{2}$, podemos reescrever (2.4) da seguinte forma

$$|(a - x_0 + x_0 - x)^2 - m(b - y_0 + y_0 - y)^2| < 1.$$

Fazendo $a' = |a - x_0|, b' = |b - y_0|, x' = x_0 - x$ e $y' = y_0 - y$, temos

$$|(a' - x')^2 - m(b' - y')^2| < 1.$$

Omitindo as linhas para simplicidade de notação, podemos supor que em (2.4) temos $0 \leq a \leq \frac{1}{2}$ e $0 \leq b \leq \frac{1}{2}$.

Agora, se $m \equiv 1 (mod\ 4)$, podemos escrever o elemento $\delta = x + y\xi \in O(m)$, com $x, y \in \mathbb{Z}$, da seguinte forma

$$x + y\xi = x + y\left(\frac{1 + \sqrt{m}}{2}\right) = x + \frac{y}{2} + \frac{y}{2}\sqrt{m}. \tag{2.5}$$

Assim, queremos encontrar $q = x + \frac{y}{2} + \frac{y}{2}\sqrt{m} \in O(m)$ tal que

$$|N(\gamma - \delta)| = \left|\left(a - x - \frac{y}{2}\right)^2 - m\left(b - \frac{y}{2}\right)^2\right| < 1$$

ou ainda

$$|N(\gamma - \delta)| = \left|(a - x - \frac{y}{2})^2 - \frac{m}{4}(2b - y)^2\right| < 1 \tag{2.6}$$

Vamos agora considerar $x_0, y_0 \in \mathbb{Z}$ tais que $|a - x_0| \leq \frac{1}{2}$ e $|b - y_0| \leq \frac{1}{4}$. Considerando $a' = |a - x_0|, b' = |2b - 2y_0|, x' = x - x_0 + y_0$ e $y' = 2y_0 - y$ e reescrevendo (2.6) temos:

$$\left|(a + x_0 - x_0 - x - \frac{y}{2})^2 - \frac{m}{4}(2b - 2y_0 + 2y_0 - y)^2\right| < 1$$

$$\left|(a' + x_0 - x - \frac{y'}{2} - y_0)^2 - \frac{m}{4}(b' - y')^2\right| < 1$$

$$\left|(a' - x' - \frac{y'}{2})^2 - \frac{m}{4}(b' - y')^2\right| < 1$$

Omitindo as linhas, pra simplificar a notação, (2.6) pode ser escrita da forma

$$\left|(a - x - \frac{y}{2})^2 - \frac{m}{4}(b - y)^2\right| < 1, \tag{2.7}$$

com $0 \leq a \leq \frac{1}{2}$ e $0 \leq b \leq \frac{1}{2}$.

As desigualdades (2.4) e (2.7) podem ser escritas como

$$|(a - x - \lambda y)^2 - n(b - y)^2| < 1, \tag{2.8}$$

com $0 \leq a \leq \frac{1}{2}$ e $0 \leq b \leq \frac{1}{2}$, onde $\lambda = 0$ e $n = m$, para $m \equiv 2, 3(mod\ 4)$, e $\lambda = \frac{1}{2}$ e $n = \frac{m}{4}$ se $m \equiv 1(mod\ 4)$.

Vamos mostrar que para $n < 8$ a desigualdade (2.8) tem solução em termos de x e y. A condição de $n < 8$ vale para $m = 6, 7$ se $m \equiv 2, 3(mod\ 4)$, e para $m = 17, 21, 29$ se $m \equiv 1(mod\ 4)$.

Vamos provar que tomado $y = 0$, um dos três valores de x, $x = 1, x = 0$ ou $x = -1$, vai satisfazer a desigualdade (2.8), isto é,

$$-1 < (a - x - \lambda y)^2 - n(b - y)^2 < 1$$

De fato, essas desigualdades podem ser escritas da seguinte forma

$$P(x, y) : (a - x - \lambda y)^2 < 1 + n(b - y)^2$$

$$Q(x, y) : n(b - y)^2 < 1 + (a - x - \lambda y)^2$$

Se $a = b = 0$,vamos ter $x = y = 0$. Caso contrário, sejam a e b ambos não nulos. Vamos mostrar que as desigualdades de pelo menos um dos seguintes pares $P(-1, 0)$ e $P(-1, 0)$, $P(0, 0)$ e $Q(0, 0)$ ou $P(1, 0)$ e $Q(1, 0)$ são válidas e assim encontramos x, y que satisfaz (2.8). Daí, temos

$$P(-1, 0) : (1 + a)^2 < 1 + nb^2$$

$$P(0, 0) : a^2 < 1 + nb^2$$

$$P(1, 0) : (1 - a)^2 < 1 + nb^2$$

$$Q(-1, 0) : nb^2 < 1 + (1 + a)^2$$

$$Q(0, 0) : nb^2 < 1 + a^2$$

$$Q(1, 0) : nb^2 < 1 + (1 - a)^2$$

Como $0 \leq a \leq \frac{1}{2}$, $n > 0$ e a e b são não ambos nulos, resultando que $P(0, 0)$ e $P(1, 0)$ são verdadeiros, vamos supor que $Q(0, 0)$ e $Q(1, 0)$ sejam falsos e vamos concluir que $P(-1, 0)$ e $Q(-1, 0)$ são verdadeiras.

Suponha que $P(-1,0)$ é falso. Como $Q(1,0)$, por hipótese, é falso , temos

$$(1+a)^2 \geq 1+nb^2 \quad \text{e} \quad 1+nb^2 \geq 1+1+(1-a)^2 = 2+(1-a)^2. \tag{2.9}$$

Juntando as desigualdades (2.9), obtemos $(1+a)^2 \geq 2+(1-a)^2$ o que implica em $a \geq \frac{1}{2}$. Como estamos supondo $0 \leq a \leq \frac{1}{2}$, segue que $a = \frac{1}{2}$. Substituindo a em (2.9), obtemos

$$\frac{9}{4} \geq 1+nb^2 \geq \frac{9}{4}$$

e portanto $nb^2 = \frac{5}{4}$. Mas, pelo lema que provaremos a seguir, $nb^2 = \frac{5}{4}$ não é possível. Assim, $P(-1,0)$ é verdadeira.

Além disso, $Q(-1,0)$ é $nb^2 < 1+(1+a)^2$. Como $n < 8$ e $b^2 \leq \frac{1}{4}$, temos $nb^2 < 8\frac{1}{4} \leq 1+(1+a)^2$ e portanto $Q(-1,0)$ é verdadeira, concluindo a demonstração.

■

Lema 2.2.8. *$nb^2 = \frac{5}{4}$ não pode acontecer.*

Demonstração. Suponha que a igualdade vale. Supondo inicialmente que $m \equiv 2,3(mod\ 4)$. Neste caso, como $n = m$ e escrevendo $b = \frac{p}{q}$, com $mdc(p,q) = 1$, temos $4mp^2 = 5q^2$ e portando $p^2|5q^2$. Como p e q são primos entre si, então $p^2|5$ e consequentemente $p = \pm 1$. Assim, $4m = 5q^2$ e portanto $q^2|4m$. Como m é livre de quadrados, resulta $q = \pm 2$. Segue que $4m = 5.4$ e assim $m = 5 \equiv 1(mod\ 4)$, o que é uma contradição.

Suponha agora que $m \equiv 1(mod\, 4)$. Neste caso, $m = 4n$, logo $mb^2 = 5$. Como acima, escrevendo $b = \frac{p}{q}$ com p e q primos entre si, temos $m\frac{p^2}{q^2} = 5$, o que implica em $mp^2 = 5q^2$ e assim $p^2|5q^2$. Como p e q são primos entre si, segue que $p^2|5$ e assim $p = \pm 1$. Temos então $5q^2 = m$ e portanto $q^2|m$, e como m é livre quadrados, temos $q = \pm 1$. Logo, $b = \pm 1$, contradizendo $0 \leq b \leq \frac{1}{2}$.

■

Observação 2.2.9. *Ao contrário do Teorema 2.2.3 que determina um quociente e o resto da divisão euclidiana, na demonstração do Teorema 2.2.7 encontramos o valor de $y = y_0$ e três possíveis valores de x, denotados por: $x_0 = x_0$, $x_{-1} = x_0 - 1$ e $x_1 = x_0 + 1$, tais que pelo menos um dos pares $q_i = x_i + y\sqrt{m}$ e $r_i = \alpha - q_i\beta$, com $i = -1, 0, 1$, vai satisfazer a condição do algoritmo da divisão.*

A seguir vamos mostrar exemplos que ilustram a aplicação do algoritmo.

Exemplo 2.2.10. *Sejam* $m = 7$, $\alpha = 114 + 200\sqrt{7}$ *e* $\beta = 45$. *Neste caso,* $m \equiv 3(mod\ 4)$ *e assim* $O(7) = \mathbb{Z}[\sqrt{7}]$. *Vamos encontrar* $q = x + y\sqrt{7}$, $r = s + t\sqrt{7} \in O(7)$ *tais que* $\alpha = q\beta + r$ *com* $|N(r)| < |N(\beta)|$. *Escrevendo* $\dfrac{\alpha}{\beta} = a + b\sqrt{7} = \dfrac{114}{45} + \dfrac{200}{45}\sqrt{7}$, *e vamos tomar* $x_0, y \in \mathbb{Z}$ *tais que* $|a - x_0| \leq \dfrac{1}{2}$ *e* $|b - y| \leq \dfrac{1}{2}$. *Escolhendo* $x_0 = 3$ *e* $y = 4$, *temos*

$$|a - x_0| = \left|\frac{114}{45} - 3\right| = \left|\frac{-21}{45}\right| \leq \frac{1}{2}$$

e

$$|b - y| = \left|\frac{200}{45} - 4\right| = \left|\frac{20}{45}\right| \leq \frac{1}{2}$$

Assim, já temos o valor de $y = y_0 = 4$ *e três candidatos para* x *que são*

$$x_{-1} = x_0 - 1 = 2, \quad x_0 = 3 \quad ou \quad x_1 = x_0 + 1 = 4.$$

Pelo menos um dos valores vai verificar o algoritmo da divisão. Sejam $q_i = x_i + y\sqrt{7}$ *e* $r_i = \alpha - q_i\beta$, $i = -1, 0, 1$. *Vamos verificar qual dos* $r_i's$ *satisfaz a condição* $|N(r_i)| < |N(45)|$.

$$r_{-1} = 144 + 200\sqrt{7} - (2 + 4\sqrt{7}) \cdot 45 = 54 + 20\sqrt{7} \Rightarrow N(r_{-1}) = 116.$$

$$r_0 = 144 + 200\sqrt{7} - (3 + 4\sqrt{7}) \cdot 45 = 9 + 20\sqrt{7} \Rightarrow N(r_0) = -2719.$$

$$r_1 = 144 + 200\sqrt{7} - (4 + 4\sqrt{7}) \cdot 45 = -36 + 20\sqrt{7} \Rightarrow N(r_1) = -1504.$$

Como $N(45) = 2025$, *os únicos* $r_i's$ *que satisfazem a condição do algoritmo da divisão são* r_{-1} *e* r_1. *Logo os valores procurados para* q *e* r *são:* $q = q_{-1} = 2 + 4\sqrt{7}$ *e* $r = r_{-1} = 54 + 20\sqrt{7}$; $q = q_1 = 4 + 4\sqrt{7}$ *e* $r = r_1 = -36 + 20\sqrt{7}$.

Exemplo 2.2.11. *Sejam* $m = 29$, $\alpha = 42 + 66\sqrt{29}$ *e* $\beta = 5$. *Como* $29 \equiv 1(mod\ 4)$, *então* $O(29) = \mathbb{Z}\left[\dfrac{1 + \sqrt{29}}{2}\right]$. *Vamos encontrar* $q = x + y\sqrt{29}, r = s + t\sqrt{29} \in O(29)$ *tais que* $\alpha = q\beta + r$ *com* $||N(r)|| < ||N(5)||$. *Escrevendo* $\dfrac{\alpha}{\beta} = a + b\sqrt{29} = \dfrac{42}{5} + \dfrac{66}{5}\sqrt{29}$, *vamos tomar inicialmente* $y = \dfrac{v}{2}$ *com* $v \in \mathbb{Z}$ *tal que* $||b - y|| \leq \dfrac{1}{4}$. *Seja* $y = \dfrac{26}{2} = 13$. *Neste caso,*

$$||b - y|| = \left|\left|\frac{66}{5} - 13\right|\right| = \frac{1}{5} \leq \frac{1}{4}$$

Com $y \in \mathbb{Z}$, *vamos tomar agora* $x_0 \in \mathbb{Z}$ *tal que* $||a - x_0|| \leq \dfrac{1}{2}$. *Escolhendo* $x_0 = 8$, *temos*

$$||a - x_0|| = \left|\left|\frac{42}{5} - 8\right|\right| = \frac{2}{5} \leq \frac{1}{2}$$

Assim, já temos o valor de y *e três candidatos para* x *que são:*

$$x_{-1} = x_0 - 1 = 7, \quad x_0 = 8 \quad e \quad x_1 = x_0 + 1 = 9.$$

Pelo menos um deles vai atender às condições do algoritmo da divisão. Sejam $q_i = x_i + y\sqrt{29}$ *e* $r_i = \alpha - q_i\beta, i = -1, 0, 1$. *Testando então:*

$$r_{-1} = 42 + 66\sqrt{29} - (7 + 13\sqrt{29}) \cdot 5 = 7 + \sqrt{29} \Rightarrow N(r_{-1}) = 20.$$

$$r_0 = 42 + 66\sqrt{29} - (8 + 13\sqrt{29}) \cdot 5 = 2 + \sqrt{29} \Rightarrow N(r_{-1}) = 25.$$

$$r_1 = 42 + 66\sqrt{29} - (9 + 13\sqrt{29}) \cdot 5 = -3 + \sqrt{29} \Rightarrow N(r_{-1}) = 20.$$

Como $N(5) = 25$, *então* r_{-1} *e* r_1 *satisfazem as condições do algoritmo da divisão. Logo, encontramos dois possíveis valores para* q *e* r: $q = q_{-1} = 7 + 13\sqrt{29}, r = r_{-1} = 7 + \sqrt{29}$ *e* $q = q_1 = 9 + 1\sqrt{29}, r = r_1 = -3 + \sqrt{29}$.

Exemplo 2.2.12. $O(23)$ *não é um anel euclidiano com a norma* $|N|$. *Vamos supor que* $O(23)$ *seja um anel euclidiano com a norma* $|N|$. *Sejam* $\alpha = 7$ *e* $\beta = \sqrt{23}$. *Temos que encontrar* $q, r \in O(23)$ *tais que* $\alpha = q\beta + r$ *com* $|N(r)| < |N(\sqrt{23})| = 23$. *Mas, como vimos no Lema 2.2.1, isto é equivalente a encontrar* $q = x + y\sqrt{23}$ *tal que*

$$\left| N\left(\frac{\alpha}{\beta} - q\right)\right| < 1,$$

ou ainda,

$$\left| N\left(q - \frac{\alpha}{\beta}\right)\right| < 1,$$

Como $\dfrac{\alpha}{\beta} = \dfrac{7}{23}\sqrt{23}$ *e* $q = x + y\sqrt{23}$, *temos que encontrar* $x, y \in \mathbb{Z}$ *tais que*

$$\left| N\left(x - \left(\frac{7}{23} - y\right)\sqrt{23}\right)\right| < 1,$$

isto é,

$$|23x^2 - (7 - 23y)^2| < 23.$$

Seja $t = 23x^2 - (7 - 23y)^2 = 23x^2 - z^2$, *onde* $z = 7 - 23y$. *Então* $t \equiv -49 \equiv -3 (mod\ 23)$. *Como* $|t| < 23$ *temos que ter* $t = -3$ *ou* $t = 20$.

Se $t = -3$, *temos* $23x^2 - (7 - 23y)^2 = -3$. *Segue que nem* x *nem* z *podem ser divisíveis por* 3. *Tomando congruência módulo 3, temos* $t = -3 \equiv 0 (mod\ 3)$. *Como* $x^2 \equiv z^2 \equiv 1 (mod\ 3)$, *já que* x *e* z *não são divisíveis por 3, segue que* $t = 23x^2 - z^2 \equiv 23 - 1 \equiv 22 \equiv 1 (mod\ 3)$. *Contradição.*

Analogamente, se $t = 20$, *temos* $23x^2 - z^2 = 20$. *Segue que nem* x *nem* z *podem ser divisíveis por 5. Tomando congruência módulo 5, temos* $t = 20 \equiv 0 (mod\ 5)$. *Como* $x^2 \equiv \pm 1 (mod\ 5)$ *e* $z^2 \equiv \pm 1 (mod\ 5)$, *em qualquer caso, temos* $t = 23x^2 - z^2 \equiv 3x^2 - z^2 \not\equiv 0 (mod\ 5)$. *Contradição.*

Assim, como não foi possível encontrar $q, r \in O(23)$ *tais que* $\alpha = q\beta + r$ *com* $|N(r)| < |N(\sqrt{23})| = 23$, *então* $O(m)$ *não é um anel euclidiano com a norma* $|N|$.

A prova de que só existem os 16 valores positivos de m mencionados anteriormente para os quais $O(m)$ é euclidiano com a norma euclidiana $|N|$ foi dada depois que H. Denvenport mostrou em [12] que $O(m)$ não pode ser euclidiano para a norma $||N||$ se $m > 2^{14}$. Para finalizar a seção, vamos apresentar a seguir uma demonstração parcial desse fato.

Teorema 2.2.13. *Existe somente um número finito de valores de $m > 0$ e $m \not\equiv 1(mod\ 4)$ para os quais $O(m)$ é euclidiano para $||N||$.*

Demonstração. Seja $m > 0$ e $m \not\equiv 1(mod\ 4)$ tal que $O(m)$ seja euclidiano para $||N||$. Na desigualdade (2.1) do Teorema 2.2.6 vamos fazer $a = 0$ e $b = t/m$, onde $t \in \mathbb{Z}$ será determinado oportunamente. Logo devem existir $r, s \in \mathbb{Z}$ tais que $||r^2 - m(t/m - s)^2|| < 1$. Reescrevemos essa desigualdade como $||(ms-t)^2 - mr^2|| < m$. Como $(ms-t)^2 - mr^2 \equiv t^2(mod\ m)$, concluímos que existem inteiros x e z tais que

$$z^2 - mx^2 \equiv t^2(mod\ m) \tag{2.10}$$

e

$$||z^2 - mx^2|| < m. \tag{2.11}$$

Se $m \equiv 3(mod\ 4)$, vamos escolher t que seja ímpar e $5m < t^2 < 6m$. Mostraremos mais a frente que existe uma quota M tal que para todo $m > M$ existe t verificando as condições acima.

Por (2.11), $-m < z^2 - mx^2 < m$. Logo

$$-7m < -m - t^2 < (z^2 - mx^2) - t^2 < m - t^2 < -4m.$$

Tome $e = (z^2 - mx^2) - t^2$. Temos então que $-7m < e < -4m$ e e é múltiplo de m. Logo os únicos valores possíveis para e são $-6m$ ou $-5m$, isto é, $z^2 - mx^2 = t^2 - 5m$ ou $z^2 - mx^2 = t^2 - 6m$. Podemos deduzir das duas alternativas que

$$t^2 - z^2 = m(5 - x^2) \quad \text{ou} \quad t^2 - z^2 = m(6 - x^2).$$

Vamos a seguir tomar resíduos módulo 8. Como t é ímpar, $t^2 \equiv 1(mod\ 8)$. Para os outros valores temos $z^2, x^2 \equiv 0, 1, 4(mod\ 8)$ e, como $m \equiv 3(mod\ 4)$, então $m \equiv 3, 7(mod\ 8)$. Portanto $t^2 - z^2 \equiv 0, 1, 5(mod\ 8)$. Por outro lado, $5 - x^2 \equiv 1, 4, 5(mod\ 8)$. Logo $m(5 - x^2) \equiv 3, 4, 7(mod\ 8)$ (nos dois casos possíveis, $m \equiv 3(mod\ 8)$ ou $m \equiv 7(mod\ 8)$). Comparando os possíveis valores de $z^2 - t^2$ e $m(5 - x^2)$ módulo 8, vemos que $z^2 - t^2 = m(5 - x^2)$ não pode ocorrer. Procedendo da mesma maneira com $m(6-x^2)$, obtemos que módulo 8 assumirá um dos valores $2, 3, 6$ ou 7. Como nenhum desses valores pode ser assumido por $t^2 - z^2$, obtemos que $t^2 - z^2 = m(6 - x^2)$ também não pode ocorrer.

Para finalizar a demonstração no caso $m \equiv 3(mod\ 4)$ só nos falta mostrar existência da quota M, conforme afirmamos acima. Vamos fazer $t = 2c + 1$. Para obter $5m < t^2 < 6m$ devemos ter

$$5m < (2c + 1)^2 < 6m.$$

Como podemos considerar somente valores positivos de c obtemos como solução $(-1 + \sqrt{5m})/2 < c < (-1 + \sqrt{6m})/2$. Vemos assim que só precisamos que exista um número inteiro c neste intervalo. Para que isso ocorra basta que a diferença entre os extremos do intervalo seja maior que 1, isto é,

$$(-1 + \sqrt{6m})/2 - (-1 + \sqrt{5m})/2 > 1,$$

o que nos dá $\sqrt{6m} - \sqrt{5m} > 2$. Resolvendo-se essa última desigualdade obtemos como solução $m > 44 + 8\sqrt{80} = M$.

No caso $m \equiv 2(mod\ 4)$, escolhemos t ímpar tal que $2m < t^2 < 3m$. Como no caso anterior, obteremos $t^2 - z^2 = m(2 - x^2)$ ou $t^2 - z^2 = m(3 - x^2)$. Novamente tomamos os valores acima módulo 8 e, como no caso anterior, chegamos à impossibilidade, para m suficientemente grande.

■

2.3 Exemplo de anel principal que não é euclidiano

Nessa seção vamos mostrar um contra-exemplo para a recíproca do Teorema 2.1.6, ou seja, apresentaremos um exemplo de um anel principal que não é euclidiano. Pelo visto na Seção 2.2.1, o anel $O(-19)$ não é euclidiano. Vamos mostrar que $O(-19)$ é um anel principal. Para isso, precisamos definir o que é um anel quase euclidiano.

Definição 2.3.1. *Um anel A é dito anel quase euclidiano se existe uma aplicação $m : A-\{0\} \to \mathbb{N}$ com a seguinte propriedade: para quaisquer $\alpha, \beta \in A - \{0\}$ tais que $m(\alpha) \geq m(\beta)$, temos que $\beta|\alpha$ ou existem $x, y \in A$ tais que $0 < m(x\alpha - y\beta) < m(\beta)$.*

Observação 2.3.2. *Segue da definição que $x\alpha - y\beta \neq 0$.*

O próximo resultado nos fornece a relação entre anéis quase euclidianos e anéis principais.

Teorema 2.3.3. *Todo anel quase euclidiano é principal.*

Demonstração. Seja I um ideal não nulo de A. Considere $\beta \in I$ um elemento não nulo tal que $m(\beta)$ seja mínimo entre todos os elementos não nulos de I. Vamos mostrar que β gera I, isto é, $I =< \beta >$. Lógico, $< \beta > \subset I$. Seja $\alpha \in I$ e suponha que $\alpha \notin < \beta >$. Temos que $m(\beta) \leq m(\alpha)$ e como $\alpha \notin < \beta >$, tem-se $\beta \nmid \alpha$. Como A é quase euclidiano, existem $x, y \in A$ tais que $0 < m(x\alpha - y\beta) < m(\beta)$, mas $x\alpha - y\beta \in I - \{0\}$, o que contraria a minimalidade de $m(\beta)$. Assim,$I \subseteq < \beta >$ e portanto $I =< \beta >$, isto é, A é um anel principal. ■

Teorema 2.3.4. *$O(-19)$ é um anel quase euclidiano e portanto principal.*

Demonstração. Vamos mostrar que $O(-19)$ é quase euclidiano com a função $m(\alpha) = ||N(\alpha)||$. Como $-19 \equiv 1(mod\ 4)$, então

$$O(-19) = \left\{ \frac{a + b\sqrt{-19}}{2}, \quad \text{com} \quad a, b \in \mathbb{Z} \quad \text{e} \quad a \equiv b\ (mod\ 2) \right\}.$$

Dados $\alpha, \beta \in O(-19) - \{0\}$ tais que $N(\alpha) \geq N(\beta)$, suponha que $\beta \nmid \alpha$. Queremos encontrar $x, y \in O(-19)$ tais que $0 < ||N(x\alpha - y\beta)|| < ||N(\beta)||$. De modo análogo ao Lema 2.2.1, isso é equivalente a encontrar $x, y \in O(-19)$ tais que

$$0 < \left| N\left(x\frac{\alpha}{\beta} - y \right) \right| < 1.$$

Observe que $\frac{\alpha}{\beta} \in \mathbb{Q}[\sqrt{-19}]$ e $\frac{\alpha}{\beta} \notin O(-19)$. Podemos escrever $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-19}}{c}$, onde $a, b, c \in \mathbb{Z}$, $mdc(a, b, c) = 1$ e $c > 1$. Vamo considerar 4 casos para c:

1. $c = 2$: como $\frac{\alpha}{\beta} \notin O(-19)$, então a e b têm paridades distintas. Considere $x = 1$ e $y = \frac{a-1+b\sqrt{-19}}{2} \in O(-19)$, temos

$$x\frac{\alpha}{\beta} - y = \frac{a+b\sqrt{-19}}{2} - \frac{a-1+b\sqrt{-19}}{2} = \frac{1}{2} \neq 0$$

e temos

$$0 < \left| N\left(x\frac{\alpha}{\beta} - y\right)\right| = \left|N\left(\frac{1}{2}\right)\right| = \left|\frac{1}{4}\right| < 1$$

2. $c = 3$: como $mdc(a, b, c) = 1$, então a e b não podem ser ambos divisíveis por 3, e então $a^2 + b^2 \equiv 1(mod\ 3)$ ou $a^2 + b^2 \equiv 2\ (mod\ 3)$. Como $19 \equiv 1\ (mod\ 3)$, então $a^2 + 19b^2 \equiv a^2 + b^2 \equiv 1\ (mod\ 3)$ ou $a^2 + 19b^2 \equiv a^2 + b^2 \equiv 2\ (mod\ 3)$. Daí existem $q, r \in \mathbb{Z}$ tais que $a^2 + 19b^2 = 3q + r$, com $r = 1$ ou $r = 2$. Tomando $x = a - b\sqrt{-19}$ e $y = q$ em $O(-19)$, temos

$$\begin{aligned} x\frac{\alpha}{\beta} - y &= (a - b\sqrt{-19})\left(\frac{a+b\sqrt{-19}}{3}\right) - q \\ &= \frac{a^2+19b^2}{3} - q \\ &= \frac{1}{3}(a^2 + 19b^2 - 3q) \\ &= \frac{r}{3} \\ &\neq 0 \end{aligned}$$

e

$$0 < \left| N\left(x\frac{\alpha}{\beta} - y\right)\right| = \left|N\left(\frac{r}{3}\right)\right| \leq \left|\frac{4}{9}\right| < 1$$

3. $c = 4$: como $mdc(a, b, c) = 1$, então a e b não podem ser ambos pares. Suponha que a e b têm paridades diferentes. Se a é par e b é ímpar, então $a^2 \equiv 0\ (mod\ 4)$ e $b^2 \equiv 1\ (mod\ 4)$, e como $19 \equiv 3(mod\ 4)$, temos que $a^2 + 19b^2 \equiv 3\ (mod\ 4)$. Analogamente, se a é ímpar e b é par, então $a^2 + 19b^2 \equiv 1\ (mod\ 4)$. Portanto existem $q, r \in \mathbb{Z}$ tais que $a^2 + 19b^2 = 4q + r$,

onde $r = 1$ ou $r = 3$. Assim, tomando $x = a - b\sqrt{-19}$ e $y = q$ em $O(-19)$, temos

$$\begin{aligned} x\frac{\alpha}{\beta} - y &= (a - b\sqrt{-19})\left(\frac{a + b\sqrt{-19}}{4}\right) - q \\ &= \frac{a^2 + 19b^2}{4} - q \\ &= \frac{1}{4}(a^2 + 19b^2 - 4q) \\ &= \frac{r}{4} \\ &\neq 0 \end{aligned}$$

e

$$0 < \left|N\left(x\frac{\alpha}{\beta} - y\right)\right| = \left|N\left(\frac{r}{4}\right)\right| \leq \left|\frac{9}{16}\right| < 1$$

Suponha agora que a e b sejam ambos ímpares. Como $a^2 \equiv b^2 \equiv 1(mod\ 8)$, então $a^2+19b^2 \equiv a^2+3b^2 \equiv 4(mod\ 8)$ e assim existe $q \in \mathbb{Z}$ tal que $a^2+19b^2 = 8q+4$. Tomando $x = \dfrac{a - b\sqrt{-19}}{2}$ e $y = q$ em $O(-19)$, temos

$$\begin{aligned} x\frac{\alpha}{\beta} - y &= \left(\frac{a - b\sqrt{-19}}{2}\right)\left(\frac{a + b\sqrt{-19}}{4}\right) - q \\ &= \frac{a^2 + 19b^2}{8} - q \\ &= \frac{1}{8}(a^2 + 19b^2 - 8q) \\ &= \frac{1}{2} \\ &\neq 0 \end{aligned}$$

e

$$0 < \left|N\left(x\frac{\alpha}{\beta} - y\right)\right| = \left|N\left(\frac{1}{2}\right)\right| \leq \left|\frac{1}{4}\right| < 1$$

4. $c \geq 5$: Como $mdc(a, b, c) = 1$, existem $d, e, f \in \mathbb{Z}$ tais que

$$ad + be + cf = 1. \tag{2.12}$$

Dividindo $ae - 19bd$ por c existem $q, r \in \mathbb{Z}$ tais que

$$ae - 19bd = qc + r \tag{2.13}$$

com $|r| \leq \frac{c}{2}$. Tomando $x = e + d\sqrt{-19}$ e $y = q - f\sqrt{-19}$ em $O(-19)$, temos:

$$\begin{aligned} x\frac{\alpha}{\beta} - y &= \left(e + d\sqrt{-19}\right)\left(\frac{a + b\sqrt{-19}}{c}\right) - (q - f\sqrt{-19}) \\ &= \frac{ae - 19bd + (ad + be)\sqrt{-19}}{c} - (q - f\sqrt{-19}) \\ &= \frac{1}{c}(ae - 19bd - qc + (ad + be + cf)\sqrt{-19}) \\ &= \frac{1}{c}(r + \sqrt{-19}) \\ &\neq 0 \end{aligned}$$

onde a última igualdade vem de (2.12) e (2.13). Assim $|N(x\frac{\alpha}{\beta} - y)| > 0$.

Por fim, vejamos que $|N(x\frac{\alpha}{\beta} - y)| < 1$. Se $c = 5$, então $|r| \leq 2$ e

$$\left|N\left(x\frac{\alpha}{\beta} - y\right)\right| = \left|N\left(\frac{1}{c}(r + \sqrt{-19})\right)\right| = \left|\frac{1}{25}(r^2 + 19)\right| \leq \frac{1}{25}(4 + 19) = \frac{23}{25} < 1$$

Se $c \geq 6$, então $|r| \leq \frac{c}{2}$ e

$$\left|N\left(x\frac{\alpha}{\beta} - y\right)\right| = \left|N\left(\frac{1}{c}(r + \sqrt{-19})\right)\right| \leq \frac{1}{4} + \frac{19}{c^2} \leq \frac{1}{4} + \frac{19}{36} = \frac{28}{36} = \frac{7}{9} < 1.$$

■

Capítulo 3

Unidades do Anel dos Inteiros Quadráticos

Neste capítulo vamos estudar as unidades do anel dos inteiros quadráticos. O estudo está divido nos casos real e imaginário. No caso imaginário veremos que o grupo multiplicativo das unidades de $O(m)$ é finito. Já no caso real, o o grupo multiplicativo das unidades é infinito e "gerado"por uma unidade $u_0 \in \emptyset(m)$, chamada de unidade fundamental.

3.1 Unidades em $O(m)$

Dados $\alpha, \beta \in O(m) - \{0\}$ diremos α e β serão associados se $\alpha \mid \beta$ e $\beta \mid \alpha$. Os elementos que são associados a 1 são chamados *unidades* de $O(m)$. Vemos que $u \in O(m)$ é associada 1 quando existe $u' \in O(m)$ tal que $uu' = 1$, isto é, $u^{-1} = u' \in O(m)$. Vamos denotar por $O(m)^*$ o conjunto das unidades de $O(m)$. Note que o produto de duas unidades é ainda uma unidade e $O(m)^*$ é um subgrupo do grupo multiplicativo de $\mathbb{Q}[\sqrt{m}]$.

Observação 3.1.1. *Note que se $u \in O(m)^*$, então $N(u) = \pm 1$. De fato, se $u \in O(m)^*$, então existe $u' \in O(m)$ tal que $uu' = 1$. Assim, $N(uu') = N(1) = 1$. Pela Proposição 1.1.10 - (c), temos*

$$N(u)N(u') = 1.$$

Com $N(u), N(u') \in \mathbb{Z}$, então $N(u) = N(u') = 1$ ou $N(u) = N(u') = -1$. Logo, $N(u) = \pm 1$.

Vamos classificar as unidades de $O(m)$ conforme o valor de sua norma. Dizemos que $u \in O(m)^*$ é *própria* se $N(u) = 1$ e que é *imprópria* se $N(u) = -1$. Como $N(-1) = N(1) = 1$, então 1 e -1 são unidades próprias e assim unidades próprias sempre existem. Já unidades impróprias podem não ocorrer. Observe que se $m < 0$ e $\alpha = a + b\sqrt{m} \in O(m)$, então

$$N(\alpha) = a^2 + b^2||m|| > 0.$$

Assim, $N(\alpha) = -1$ não pode ocorrer. Logo, $O(m)$ não possui unidades impróprias se $m < 0$.

A seguir vamos ver algumas propriedades que envolvem unidades.

Lema 3.1.2. *Sejam $\alpha, \beta \in O(m) - \{0\}$.*

(a) *$u \in O(m)^*$ se, e somente se, $|N(u)| = 1$.*

(b) *α e β são associados se, e somente se, existe $u \in O(m)^*$ tal que $\alpha = u\beta$.*

(c) *Se $\alpha|\beta$ e $|N(\alpha)| = |N(\beta)|$, então α e β são associados.*

Demonstração.

(a) Se $u \in O(m)^*$, pela Observação 3.1.1, temos que $N(u) = \pm 1$, assim $|N(u)| = 1$. Reciprocamente, se $|N(u)| = 1$, então $|u\overline{u}| = 1$ o que implica em $u\overline{u} = \pm 1$, ou $u(\pm\overline{u}) = 1$. Logo $u \in O(m)^*$, pois $\pm\overline{u} \in O(m)$.

(b) Suponha que α, β são associados. Então existem $u, u_1 \in O(m)$ tais que $\alpha = u\beta$ e $\beta = u_1\alpha$. Assim $\alpha = u(u_1\alpha)$, o que implica em $uu_1 = 1$ e u é unidade de $O(m)$ e temos $\alpha = u\beta$. Por outro lado, supondo que $\alpha = u\beta$, com $u \in O(m)^*$, então $\beta|\alpha$. Seja $u' \in O(m)$ tal que $u'u = 1$. Assim,

$$u'\alpha = u'(u\beta) = (u'u)\beta = 1\beta = \beta.$$

Logo, $\alpha|\beta$ e portanto α e β são associados.

(c) Se $\alpha|\beta$, então existe $u \in O(m)$ tal que $\beta = u\alpha$. Daí, $|N(\beta)| = |N(u)||N(\alpha)|$, e como $|N(\alpha)| = |N(\beta)|$, segue que $|N(u)| = 1$. De (a) e (b) concluímos que α e β são associados.

■

Exemplo 3.1.3. *Tomando $m = 2$, temos que $N(1 + \sqrt{2}) = 1^2 - 2 = -1$, e assim $1 + \sqrt{2}$ é uma unidade imprópria de $O(2)$. Por outro lado, tomando $m = 3$ vemos que $O(3)$ não tem unidades impróprias, isto porque $\alpha = a + b\sqrt{3}$ é uma unidade imprópria se, e somente se, $N(\alpha) = -1$, e assim deveríamos ter $a^2 - 3b^2 = -1$, o que resultaria em $a^2 \equiv -1 (mod\ 3)$, o que não poderia acontecer.*

3.2 As Unidades do Anel dos Inteiros Quadráticos no caso complexo

A seguir vamos caracterizar as unidades de $O(m)$ com $m < 0$.

Teorema 3.2.1. (a) *Se $m = -1$, as unidades de $O(m)$ são ± 1 e $\pm\sqrt{-1}$.*

(b) *Se $m = -3$, as unidades de $O(m)$ são ± 1, $\pm\xi$ e $\pm\xi^2$, onde $\xi = \dfrac{1+\sqrt{m}}{2}$.*

(c) *Se $m < 0$ e $m \neq -1, -3$, as únicas unidades de $O(m)$ são ± 1.*

Demonstração. Seja $u = a + b\xi \in O(m)^*$

(a) Como $-1 \not\equiv 1(mod\ 4)$, então $u = a + b\sqrt{-1}$ e $N(u) = a^2 + b^2 = 1$. Portanto temos $a = \pm 1$ e $b = 0$ ou $a = 0$ e $b = \pm 1$, ou seja, $u = \pm 1$ ou $u = \pm\sqrt{-1}$.

(b) Observe que $\pm 1, \pm\xi$ e ξ^2 têm norma 1 e portanto são inversíveis. Como $-3 \equiv 1(mod\ 4)$, então

$$u = a + b\left(\frac{1+\sqrt{-3}}{2}\right) = \frac{(2a+b)}{2} + \frac{b}{2}\sqrt{-3},$$

com $a, b \in \mathbb{Z}$, e assim

$$N(u) = \frac{(2a+b)^2 + 3b^2}{4} = 1.$$

Logo, devemos ter $(2a+b)^2 + 3b^2 = 4$. Se $b \neq 0$, então $b = \pm 1$. Para $b = 1$, temos

$$(2a+1)^2 + 3 = 4 \Rightarrow (2a+1)^2 = 1 \Rightarrow 2a + 1 = \pm 1.$$

Se $2a + 1 = 1$, então $a = 0$ e se $2a + 1 = -1$, então $a = -1$. Logo, temos duas opções:
Para $b = 1$ e $a = 0$, temos

$$u = \frac{1+\sqrt{-3}}{2} = \xi.$$

e para $b = 1$ e $a = -1$, :

$$u = \frac{-1+\sqrt{-3}}{2} = \xi^2.$$

Se $b = -1$, temos

$$(2a-1)^2 + 3 = 4 \Rightarrow (2a-1)^2 = 1 \Rightarrow 2a - 1 = \pm 1.$$

Se $2a - 1 = 1$, então $a = 1$ e se $2a - 1 = -1$, então $a = 0$. Assim, temos duas opções:
Para $b = -1$ e $a = 1$, temos

$$u = \frac{1-\sqrt{-3}}{2} = -\xi^2$$

Para $b = -1$ e $a = 0$, temos

$$u = \frac{-1-\sqrt{-3}}{2} = -\xi.$$

Por fim, se $b = 0$, temos

$$(2a)^2 = 4 \Rightarrow a = \pm 1.$$

Neste caso, vamos ter $u = \pm 1$.

(c) Análogo aos itens (a) e (b), se $m \not\equiv 1(mod\ 4)$, então $u = a + b\sqrt{m}$, com $a, b \in \mathbb{Z}$, e assim

$$N(u) = a^2 + |m|b^2 = 1.$$

Se $m \leq -2$, então $b = 0$ e assim $a = \pm 1$. Logo, devemos ter $u = \pm 1$.

Se $m \equiv 1(mod\ 4)$, então $u = a + b\left(\frac{1+\sqrt{m}}{2}\right) = \frac{(2a+b)+b\sqrt{m}}{2}$ e

$$N(u) = \frac{(2a+b)^2 + |m|b^2}{4} = 1 \Rightarrow (2a+b)^2 + |m|b^2 = 4.$$

Para $m \leq -7$, devemos ter $b > 0$ e assim $a = \pm 1$, o que implica novamente em $u = \pm 1$.

■

3.3 As Unidades do Anel dos Inteiros Quadráticos no caso real

O estudo das unidades para $m > 0$ é um pouco mais complicado e será tratado a partir de agora. Neste caso, vamos mostrar que se $m > 1$, então o conjunto $O(m)^*$ é infinito e existe $u_0 \in O(m)^*$, chamada de *unidade fundamental*, tal que

$$O(m)^* = \{\pm u_0^n, n \in \mathbb{Z}\}$$

Seja $u = a + b\sqrt{m} \in O(m)^*$. Como

$$N(u) = u\overline{u} = \pm 1$$

então $u, -u, \overline{u}, -\overline{u}$ são unidades de $O(m)$. Observe que se $u \neq \pm 1$, então os elementos $u, -u, \overline{u}, -\overline{u}$ são todos distintos. A seguir vamos apresentar alguns resultados que irão nos auxiliar a caracterizar a unidade fundamental.

Lema 3.3.1. *Se $\mu = c + d\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ é uma unidade de $O(m)$ diferente de ± 1, então:*

(a) *O conjunto $\{\pm\mu, \pm\overline{\mu}\}$ tem intersecção não vazia com cada um dos seguintes intervalos $(-\infty, -1)$, $(-1, 0)$, $(0, 1)$ e $(1, \infty)$.*

(b) *$\mu > 1$ se, e somente se, $c > 0$ e $d > 0$.*

(c) *O intervalo $(1, M]$ contém apenas um número finito de unidades de $O(m)$, onde $M > 1$ é um número real.*

(d) *Se* $\mu_1 = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ *é uma outra unidade de* $O(m)$ *e* $1 < \mu$*, então* $1 < \mu_1 < \mu$ *se, e somente se,* $0 < a < c$ *e* $0 < b \leq d$*, sendo que* $b = d$ *só acontece se* $m = 5$ *e* $\mu_1 = \dfrac{1+\sqrt{5}}{2}$ *e* $\mu = \dfrac{3+\sqrt{5}}{2}$.

Demonstração.

a) Suponha, sem perda de generalidade, que $\mu > 1$, então

$$\mu = c + d\sqrt{m} > 1 \quad \text{e} \quad -\mu = -c - d\sqrt{m} < -1 \tag{3.1}$$

ou seja, $\mu \in (1, \infty)$ e $-\mu \in (-\infty, -1)$. Suponha que $N(\mu) = 1$, então

$$(c + d\sqrt{m})(c - d\sqrt{m}) = 1$$

e como $c + d\sqrt{m} > 1$, segue que

$$0 < \overline{u} = c - d\sqrt{m} < 1 \quad \text{e} \quad -1 < -\overline{u} = -c + d\sqrt{m} < 0. \tag{3.2}$$

Logo, $\overline{\mu} \in (0, 1)$ e $-\overline{\mu} \in (-1, 0)$.
Analogamente, se $N(\mu) = -1$, então

$$(c + d\sqrt{m})(c - d\sqrt{m}) = -1$$

como $c + d\sqrt{m} > 1$, segue que

$$-1 < c - d\sqrt{m} < 0 \quad \text{e} \quad 0 < -c + d\sqrt{m} < 1.$$

Assim, $\overline{\mu} \in (-1, 0)$ e $-\overline{\mu} \in (0, 1)$.

b) Suponha $\mu > 1$. Do item (a) temos que

$$c - d\sqrt{m} < c + d\sqrt{m} \Rightarrow -d < d$$

$$-c + d\sqrt{m} < c + d\sqrt{m} \Rightarrow -c < c$$

o que implica em $c > 0$ e $d > 0$. A recíproca é imediata, $c, d > \frac{1}{2}$ e $\sqrt{m} > 1$.

c) Se $\mu = c + d\sqrt{m} \in (1, M]$, temos pelo item (b) que $c > 0$ e $d > 0$. Por outro lado, $c + d\sqrt{m} \leq M$ implica $c < M$ e $d < M$, e consequentemente

$$2c < 2M \quad \text{e} \quad 2d < 2M.$$

Logo a cada unidade $\mu \in (1, M]$ corresponde um par de números inteiros $(2c, 2d) \in [1, 2M) \times [1, 2M)$. Como o número de pares inteiros nesse conjunto é finito, também o número de unidades no intervalo será finito.

d) ($\Leftarrow$) Claramente $0 < a < c$ e $0 < b \leq d$ implica em

$$0 < a < c \quad \text{e} \quad 0 < b\sqrt{m} \leq d\sqrt{m}.$$

Consequentemente, $1 < \mu_1 < \mu$.

($\Rightarrow$) Como $1 < \mu_1 < \mu$, temos $0 < \mu^{-1} < \mu_1^{-1}$. Sobre os conjugados temos que discutir duas possibilidades

$$\overline{\mu_1} > 0 \quad \text{ou} \quad \overline{\mu_1} < 0.$$

1º caso Se $\overline{\mu_1} > 0$, então $N(\mu_1) = \mu_1\overline{\mu_1} = 1$ e, pela Proposição 1.1.10 - (e), $\overline{\mu_1} = \mu_1^{-1}$. Assim

$$2\sqrt{m}(d-b) = (\mu - \mu_1) + (\overline{\mu_1} - \overline{\mu}) > 0$$

tanto para $\overline{\mu} > 0$ quanto para $\overline{\mu} < 0$. Logo $d > b$.
Por outro lado, de $N(\mu_1) = a^2 - mb^2 = 1$, temos

$$a^2 = 1 + mb^2. \tag{3.3}$$

Como $N(\mu) = c^2 - md^2 = \pm 1$, temos

$$c^2 = \pm 1 + md^2. \tag{3.4}$$

Se (3.4) é dada por $c^2 = 1 + md^2$, como $d > b > 0$, segue de (3.3) que

$$c^2 = 1 + md^2 > 1 + mb^2 = a^2$$

Logo, $c > a$, uma vez que a e c são inteiros positivos.
Se (3.4) é dado por $c^2 = -1 + md^2$, subtraindo (3.3) de (3.4) ficamos com

$$c^2 - a^2 = -1 + md^2 - 1 - mb^2 = -2 + m(d^2 - b^2).$$

Como $m \geq 2$ e $d > b$, temos $m(d^2 - b^2) > 2$, pois se $m = 2$ então $d, b \in \mathbb{Z}$ e daí $d^2 - b^2 > 1$, e se $m \geq 3$ obtemos $d^2 - b^2 \geq \frac{5}{4}$. Temos ainda $c^2 - a^2 > 0$ e assim $c > a$. Logo, se $\overline{\mu_1} > 0$, então $a < c$ e $b < d$.

2º caso Consideraremos agora o caso $\overline{\mu_1} < 0$. Logo, $N(\mu_1) = -1$ e $\mu_1^{-1} = -\overline{\mu_1}$. Temos de novo para qualquer sinal de $\overline{\mu}$ que

$$2(c-a) = (\mu - \mu_1) + (\overline{\mu} - \overline{\mu_1}) > 0$$

e dai $c > a$. Assim como caso anterior, do cálculo das normas, obtemos

$$\pm 1 + md^2 = c^2 > a^2 = -1 + mb^2.$$

Para o sinal $-$, obtemos $md^2 > mb^2$ do que resulta $d > b$. No caso $+$, temos $2 + md^2 > mb^2$, que podemos reescrever $2 > m(b+d)(b-d)$. Como $m \geq 2$ devemos ter que $(b+d)(b-d) < 1$. Observemos que se $(b+d)(b-d) \leq 0$, então $b \leq d$, como queríamos, pois b e d são positivos. Temos então que mostrar que

$$(b+d)(b-d) > 0 \tag{3.5}$$

não pode ocorrer. Suponhamos por absurdo que essa desigualdade seja verdadeira. Dela resulta que $b > d$. Consideremos as duas possibilidades para m. Se $m \not\equiv 1(mod\ 4)$, b e d são inteiros positivos. Logo $b - d \geq 1$ e $b + d > 1$, sendo uma contradição. No caso $m \equiv 1(mod\ 4)$, temos que, pelo Teorema 1.2.11, $2b$ e $2d$ são inteiros. Multiplicando a desigualdade (3.5) por 4 obtemos $(2b+2d)(2b-2d) > 0$. Agora, os termos envolvidos são inteiros e de mesma paridade. Logo $2b-2d \geq 2$ e $2b+2d \geq 2$, pois $2b > 2d > 0$. Portanto

$$(b + d)(b - d) = [(2b + 2d)(2b - 2d)]/4 \geq 1$$

e chegamos novamente a uma contradição. Portanto $b \leq d$, como queríamos.

Para completar a demonstração, observemos que $b < d$ só não ocorreu no último caso analisado, onde as condições eram: $a^2 = -1+mb^2$ e $c^2 = 1+md^2$. Novamente, utilizando o Teorema 1.2.11 multiplicamos as igualdades por 4, e levando em conta que $d = b$, obtemos

$$(2a)^2 = -4 + m(2b)^2 \quad \text{e} \quad (2c)^2 = 4 + m(2b)^2, \tag{3.6}$$

onde $2a, 2b$ e $2c$ são inteiros de mesma paridade. Deduzimos de (3.6) que

$$(2c + 2a)(2c - 2a) = (2c)^2 - (2a)^2 = 8. \tag{3.7}$$

Como $2c$ e $2a$ tem mesma paridade, $2c + 2a$ e $2c - 2a$ são pares. Como $c > a > 0$, então $2c + 2a \neq 2$. Logo em (3.7) só pode ocorrer $2c - 2a = 2$ e $2c + 2a = 4$. Resolvendo esse sistema obtemos $2c = 3$ e $2a = 1$. Usando agora (3.6), chegamos a $m(2b)^2 = 5$. Finalmente, como $m \neq 1$ obtemos $m = 5$ e $2b = 1$. Portanto

$$\mu_1 = \frac{1 + \sqrt{5}}{2} \quad \text{e} \quad \mu = \frac{3 + \sqrt{5}}{2}.$$

■

Seja $u > 1$ um número real, temos que $u^n \longrightarrow \infty$ se $n \to \infty$. Assim pelo item (a) do Lema 3.3.1 para concluir que $O(m)^*$ é infinito basta mostrar que $O(m)^* \neq \{\pm 1\}$. A prova que daremos deste resultado é devido a Dirichlet e seu principal argumento depende de uma boa aproximação, por racionais, do número irracional $\sqrt{m}$.

Lema 3.3.2. *Sejam $\alpha > 0$ um número irracional e M um inteiro positivo. Existem inteiros x, y tais que $0 < y \leq M$, $x \geq 0$ e $||x - \alpha y|| < 1/M$.*

Demonstração. Dado $t \in \mathbb{R}$, definimos $[t]$ como sendo o maior inteiro menor ou igual a t. Assim é claro que

$$0 \leq t - [t] < 1.$$

Agora dividimos o intervalo $[0, 1)$ em M subintervalos

$$[0, 1/M), [1/M, 2/M), \ldots, [(M - 1)/M, 1)$$

cada um com comprimento $1/M$. Considere os seguintes $M + 1$ números:

$$\beta_1 = \alpha - [\alpha], \beta_2 = 2\alpha - [2\alpha], \ldots, \beta_M = M\alpha - [M\alpha], \beta_{M+1} = (M + 1)\alpha - [(M + 1)\alpha].$$

Como α é irracional, temos que cada β_i satisfaz $0 < \beta_i < 1$ e assim existem inteiros $0 < u < v \leq M+1$ tais que β_u e β_v pertencem a um mesmo subintervalo, isto é,

$$|([v\alpha] - v\alpha) - ([u\alpha] - u\alpha)| = |([v\alpha] - [u\alpha]) - (v-u)\alpha| < 1/M.$$

Chamando $x = [v\alpha] - [u\alpha]$ e $y = v - u$, temos que $||x - \alpha y|| < 1/M$, com $x \geq 0$ e $0 < y \leq M$. ■

Lema 3.3.3. *Seja $\alpha > 0$ um número irracional. Existem infinitos pares de inteiros (x, y) tais que $y \neq 0$ e $|x/y - \alpha| < 1/y^2$.*

Demonstração. Primeiramente vemos que $x = [\alpha]$ e $y = 1$ satisfazem as condições do Lema. Suponhamos agora que já encontramos n pares distintos de inteiros (x_i, y_i), $i = 1, \ldots, n$ que satisfazem as condições do Lema. Tomemos

$$\delta = \min\{|x_i - \alpha y_i|, i = 1, \ldots, n\}.$$

Como α é irracional, $|x_i - \alpha y_i| > 0$ para todo i, e assim $\delta > 0$. Seja M um número natural tal que $1/M < \delta$. Pelo Lema 3.3.2, temos que existem $x, y \in \mathbb{Z}$ com $x \geq 0$ e $0 < y \leq M$ tais que $|x - \alpha y| < 1/M < \delta$. Assim, (x, y) é distinto de qualquer (x_i, y_i) e

$$|x/y - \alpha| < 1/My \leq 1/y^2.$$

Concluímos então que o conjunto de tais pares é infinito. ■

Teorema 3.3.4. *Existem inteiros x e y, com $y \neq 0$, tais que $x^2 - my^2 = 1$. Ou equivalentemente $O(m)^* \cap \mathbb{Z}[\sqrt{m}] \neq \{\pm 1\}$.*

Demonstração. Vamos começar por encontrar $k \in \mathbb{Z}$ tal que $N(\alpha) = k$ para um número infinito de elementos $\alpha \in \mathbb{Z}[\sqrt{m}]$. Sejam $x, y \in \mathbb{Z}$, com $y \neq 0$, e

$$|x/y - \sqrt{m}| < 1/y^2. \tag{3.8}$$

Temos então

$$\begin{aligned} |N(x + y\sqrt{m})| &= |x^2 - my^2| \\ &= |x - y\sqrt{m}||x + y\sqrt{m}| \\ &= y^2|x/y - \sqrt{m}||x/y + \sqrt{m}| \\ &< |x/y + \sqrt{m}| = |x/y - \sqrt{m} + 2\sqrt{m}| \\ &\leq |x/y - \sqrt{m}| + 2\sqrt{m} \\ &< 1/y^2 + 2\sqrt{m} \\ &\leq 1 + 2\sqrt{m} \end{aligned}$$

Portanto $N(x + y\sqrt{m})$ é um inteiro entre $-1 - 2\sqrt{m}$ e $1 + 2\sqrt{m}$. Como, pelo Lema 3.3.3, existem infinitos pares (x, y) que satisfazem (3.8) acima, temos que existe $k \in \mathbb{Z}$, $k \neq 0$, com $|k| < 1 + 2\sqrt{m}$ e tal que $N_k = \{\alpha \in \mathbb{Z}[\sqrt{m}] | N(\alpha) = k\}$ é um conjunto infinito.

Sejam $\alpha, \beta \in N_k$ tais que $\alpha \neq \pm\beta$. Então $\alpha\beta^{-1} \neq \pm 1$ e $N(\alpha\beta^{-1}) = N(\alpha)/N(\beta) = k/k = 1$. Assim, para concluir o resultado, basta encontrar α e β nestas condições e tais que $\alpha\beta^{-1} \in \mathbb{Z}[\sqrt{m}]$. Pela Proposição 1.1.10, temos que

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

Estamos portanto procurando $\alpha, \beta \in N_k$ tais que $\alpha\overline{\beta} \in k\mathbb{Z}[\sqrt{m}]$ e $\alpha \neq \pm\beta$. Seja

$$S_k = \{(\overline{x}, \overline{y}) \in \mathbb{Z}_{|k|} \times \mathbb{Z}_{|k|} | \alpha = x + y\sqrt{m} \in N_k\},$$

onde $\mathbb{Z}_{|k|}$ é o conjunto das classes dos inteiros módulo $|k|$. Como S_k é finito e N_k é infinito, existem $\alpha = x + y\sqrt{m}$ e $\beta = x' + y'\sqrt{m}$ em N_k tais que $\alpha \neq \pm\beta$ e $(\overline{x}, \overline{y}) = (\overline{x'}, \overline{y'})$, isto é, k divide $x - x'$ e $y - y'$. Denotando $x - x' = ka$ e $y - y' = kb$, com $a, b \in \mathbb{Z}$, temos

$$\alpha - \beta = (x - x') + (y - y')\sqrt{m} = ka + kb\sqrt{m} = k(a + b\sqrt{m}) = k\gamma \in k\mathbb{Z}[\sqrt{m}]$$

onde $\gamma = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$. Assim

$$k\gamma\overline{\beta} = (\alpha - \beta)\overline{\beta} = \alpha\overline{\beta} - k.$$

Logo, $\alpha\overline{\beta} = k(\gamma\overline{\beta} + 1) \in k\mathbb{Z}[\sqrt{m}]$ e ainda $\alpha \neq \pm\beta$, como queríamos.

■

Tendo em vista o Teorema 3.3.4 que para $m > 1$, $O(m)^*$ é infinito, vamos agora caracterizá-lo. O próximo resultado garante a existência da unidade fundamental.

Teorema 3.3.5. *Existe uma única unidade $\mu_0 > 1$ em $O(m)$ tal que toda unidade de $O(m)$ é da forma $\pm\mu_0^n$ com $n \in \mathbb{Z}$.*

Demonstração. Usando o Lema 3.3.1 - (a) e Teorema 3.3.4 podemos obter uma unidade $w = x + y\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, com $w > 1$. Além disso, pelo Lema 3.3.1 - (c), existe apenas um número finito de unidades no intervalo $(1, w]$. Tome então $\mu_0 = \min\{\mu | \mu \in O(m)^* \text{ e } \mu > 1\}$ (a existência do mínimo segue da afirmação anterior) e seja v uma unidade de $O(m)$ com $v > 1$. Como $\mu_0^k \to \infty$ com $k \in \mathbb{N}$ e $k \to \infty$, temos que existe n, com $n \geq 1$, tal que $0 < \mu_0^{n-1} < v \leq \mu_0^n$. Assim $0 < 1 < v\mu_0^{1-n} \leq \mu_0$ e, pela minimalidade de μ_0, temos $v\mu_0^{1-n} = \mu_0$ e assim $v = \mu_0^n$. Seja agora $v \neq \pm 1$ uma unidade qualquer de $O(m)$. Como um dos elementos de $\{\pm v, \pm v^{-1}\}$ é maior do que 1, então $v = \pm\mu_0^n$, com $n \in \mathbb{Z}$. A unicidade de μ_0 decorre de sua escolha.

■

A unidade μ_0 do Teorema 3.3.5 é chamada de unidade fundamental de $O(m)$.

Observação 3.3.6. *Segue do Lema 3.3.1 - (d) e do Teorema 3.3.5 que $\mu_0 = x + y\sqrt{m} \in O(m)^*$, com $\mu_0 > 1$, será a unidade fundamental de $O(m)$ se, e somente se, para qualquer outra unidade $\mu = a + b\sqrt{m} \in O(m)$ com $\mu > 1$, tivermos $x \leq a$ e $y \leq b$. A igualdade $x = a$ vai ocorrer se, e somente se, $\mu = \mu_0$, e se $x \neq a$, a igualdade $y = b$ ocorre se, e somente se, $m = 5$, e nesse caso $\mu_0 = \dfrac{1 + \sqrt{5}}{2}$ e $\mu = \mu_0^2 = \dfrac{3 + \sqrt{5}}{2}$.*

Observação 3.3.7. *Decorre do Teorema 3.3.5 que existe unidade μ tal que $N(\mu) = -1$ se, e somente se, $N(\mu_0) = -1$, isto é, existe unidade imprópria se, e somente se, μ_0 é unidade imprópria.*

Observação 3.3.8. *Sempre é possível encontrar a unidade fundamental. Quando $m \not\equiv 1(mod\ 4)$, então $O(m) = \mathbb{Z}[\sqrt{m}]$. Assim, os elementos $\mu \in O(m)^*$, com $\mu > 1$ são da forma*

$$\mu = x + y\sqrt{m}, \quad x, y \in \mathbb{Z} \quad x, y > 0$$

e tais que $N(\mu) = \pm 1$, ou seja,

$$x^2 - my^2 = \pm 1.$$

Assim, pela Observação 3.3.6, para encontrar a unidade fundamental basta encontrar o menor y, $y > 0$, tal que

$$\pm 1 + my^2 \tag{3.9}$$

seja um quadrado perfeito. Neste caso, temos que $\mu_0 = x + y\sqrt{m}$ é a unidade fundamental.

Se $m \equiv 1(mod\ 4)$, então

$$O(m) = \left\{ \frac{x + y\sqrt{m}}{2} \quad / \quad x, y \in \mathbb{Z} \quad e \quad x \equiv y(mod\ 2) \right\}.$$

Assim, as unidades de $O(m)$ maiores que 1, são da forma $\mu = \dfrac{x + y\sqrt{m}}{2}$, com $x, y \in \mathbb{Z}$, $x, y > 0$, $x \equiv y(mod\ 2)$ e $N(\mu) = \pm 1$, ou seja,

$$\frac{x^2 - my^2}{4} = \pm 1.$$

Análogo ao caso anterior, basta encontrar o menor $y > 0$ para o qual

$$\pm 4 + my^2$$

é um quadrado perfeito.

Exemplo 3.3.9. *Para $m = 2 \equiv 2(mod\ 4)$, temos*

y	$1 + 2y^2$	$-1 + 2y^2$
1	3	1

Assim, a unidade fundamental de $O(2)$ é $\mu_0 = 1 + \sqrt{2}$.

Analogamente, para $m = 3 \equiv 3(mod\ 4)$, temos

y	$1 + 3y^2$	$-1 + 3y^2$
1	4	2

Assim, a unidade fundamental de $O(3)$ é $\mu_0 = 2 + \sqrt{3}$.

Exemplo 3.3.10. *Considere* $m = 7 \equiv 3(mod\ 4)$*, alguns valores (3.9) são dadas por:*

y	$1+7y^2$	$-1+7y^2$
1	8	6
2	29	27
3	64	62

Logo, o menor valor de y *para que* $\pm 1 + 7y^2$ *seja um quadrado perfeito é* $y = 3$ *e obtemos* $x^2 = 64$*, ou seja,* $x = 8$*. Portanto, a unidade fundamental de* $O(7)$ *é* $\mu_0 = 8 + 3\sqrt{7}$*.*

O procedimento para encontrar a unidade fundamental descrito na Observação 3.3.8 não é muito efetivo, já que nem sempre é possível encontrar o valor de y rapidamente. Por exemplo, para $m = 31$, o menor valor de y que satisfaz (3.9) é $y = 273$. Fizemos uso de um código desenvolvido no Python, ver Apêndice A, para calcular a unidade fundamental de alguns anéis quadráticos. O resultado encontra-se na tabela abaixo:

m	Unidade Fundamental de $O(m)$
11	$10 + 3\sqrt{11}$
15	$4 + \sqrt{15}$
23	$24 + 5\sqrt{23}$
37	$6 + \sqrt{37}$
42	$13 + 2\sqrt{42}$
51	$50 + 7\sqrt{51}$
52	$649 + 90\sqrt{52}$
72	$17 + 2\sqrt{72}$

Capítulo 4

Ideais dos Anéis dos Inteiros Quadráticos

Neste capítulo vamos estudar os ideais do anel dos inteiros quadráticos. O objetivo é mostrar que os ideais de $O(m)$ se escrevem como $(vk, v(u+\xi))$ unicamente determinados por elementos $k, v \in \mathbb{Z}$, com $k, v > 0$. Por fim, definimos a norma de um ideal e mostramos que essa norma satisfaz algumas propriedade semelhantes à norma em $\mathbb{Q}[\sqrt{m}]$ definida no capítulo 1.

4.1 Os Ideais de $O(m)$

Vamos agora caracterizar os ideais de $O(m)$. Para isso recordemos que

$$O(m) = \mathbb{Z} \oplus \mathbb{Z}\xi,$$

onde $\xi = \sqrt{m}$, se $m \not\equiv 1(mod\ 4)$, e $\xi = \dfrac{1+\sqrt{m}}{2}$, se $m \equiv 1(mod\ 4)$. Pela Proposição 1.1.11, temos que ξ é raiz do polinômio $f_\xi(X) = X^2 - T(\xi)X + N(\xi)$, onde $T(\xi) = 0$ se $\xi = \sqrt{m}$ e $T(\xi) = 1$ se $\xi = \dfrac{1+\sqrt{m}}{2}$. Logo

$$\xi^2 = -N(\xi) + T(\xi)\xi. \tag{4.1}$$

Além disso, se $u \in \mathbb{Z}$, então $\overline{u} = u$ e daí

$$N(u+\xi) = (u+\xi)(u+\overline{\xi}) = u^2 + u\overline{\xi} + u\xi + \xi\overline{\xi} = u^2 + T(\xi)u + N(\xi). \tag{4.2}$$

Teorema 4.1.1. *Seja $I \neq \{0\}$ um subconjunto de $O(m)$. Então I é um ideal de $O(m)$ se, e somente se, existem inteiros k, v e u, com $v > 0$ e $k > 0$, tais que $k|N(u+\xi)$ e $I = \mathbb{Z}vk \oplus \mathbb{Z}v(u+\xi)$. Mais ainda, k e v satisfazendo tais condições são únicos.*

Demonstração.

($\Rightarrow$) Seja $I \neq \{0\}$ um ideal de $O(m)$ e $k' \in \mathbb{Z}$ tal que $k'\mathbb{Z} = I \cap \mathbb{Z}$, com $k' > 0$. Seja agora o subconjunto

$$V = \{y \in \mathbb{Z} | y > 0 \text{ e } \exists x \in \mathbb{Z} \text{ com } x + y\xi \in I\}$$

não-vazio dos naturais. Portanto existe $v > 0$ que é o menor elemento de V.

Seja $u' \in \mathbb{Z}$ tal que $u' + v\xi \in I$. Afirmamos que para todo $\alpha = a + b\xi \in I$, $a, b \in \mathbb{Z}$, tem-se que $v|b$ e $a - u'q \in I$, se $b = vq$. De fato, seja $b = vq + r$ com $q, r \in \mathbb{Z}$, $0 \leq r < v$, então

$$(a - u'q) + r\xi = \alpha - (u' + v\xi)q \in I.$$

Como $r < v$, temos $r \notin V$ e assim $r = 0$. Logo, $v|b$ e $a - u'q \in I$. Como $a - u'q \in \mathbb{Z}$ também, resulta

$$a - u'q \in I \cap \mathbb{Z} = k'\mathbb{Z} \quad \text{e} \quad a - u'q = k'c$$

com $c \in \mathbb{Z}$. Concluímos assim que

$$a + b\xi = k'c + u'q + vq\xi = k'c + q(u' + v\xi).$$

Por outro lado, como $k' \in I$, temos $k'\xi \in I$ e assim $k' = vk$ para $k \in \mathbb{Z}$. Verifiquemos agora que $v|u'$. Seja $u'\xi + v\xi^2 = (u' + v\xi)\xi \in I$, mas

$$u'\xi + v\xi^2 = u'\xi - vN(\xi) + vT(\xi)\xi = -vN(\xi) + (u' + vT(\xi))\xi$$

e assim $v|(u' + vT(\xi))$ pelo que vimos acima. Logo, $v|u'$, ou seja, $u' = vu$ com $u \in \mathbb{Z}$. Assim, $u' + v\xi = v(u + \xi)$ e um genérico $\alpha \in I$, $\alpha = a + b\xi$, será da forma

$$vkc + qv(u + \xi) \in \mathbb{Z}vk \oplus \mathbb{Z}v(u + \xi).$$

Resta mostrar que $k|N(u + \xi)$. De fato, como $N(u + \xi) = (u + \xi)(u + \overline{\xi})$, vemos que $vN(u + \xi) \in I \cap \mathbb{Z} = k'\mathbb{Z} = vk\mathbb{Z}$. Assim $vk|vN(u + \xi)$ e então $k|N(u + \xi)$, como queríamos demonstrar.

($\Leftarrow$) Seja $I = \mathbb{Z}vk \oplus \mathbb{Z}v(u + \xi)$, com k, v e u verificando as hipóteses iniciais. Para verificar que I é um ideal de $O(m)$, basta verificar que $\xi kv, \xi v(u + \xi) \in I$. De fato, temos que

$$\xi kv = kv\xi + kvu - kvu = (-u)vk + kv(u + \xi) \in \mathbb{Z}vk \oplus \mathbb{Z}v(u + \xi) = I$$

Além disso, por (4.1) e (4.2), temos

$$\begin{aligned}
\xi v(u + \xi) &= vu\xi + v\xi^2 = vu\xi + vT(\xi)\xi - vN(\xi) \\
&= vu\xi + vT(\xi)\xi - vN(\xi) - vu^2 + vu^2 - vuT(\xi) + vuT(\xi) \\
&= -vu^2 - vuT(\xi) - vN(\xi) + vu^2 + vuT(\xi) + vu\xi + vT(\xi)\xi \\
&= -v(u^2 + uT(\xi) + N(\xi)) + v(u^2 + u\xi + uT(\xi) + T(\xi)\xi) \\
&= -vN(u + \xi) + v(u + T(\xi))(u + \xi) \\
&= -vkc + v(u + T(\xi))(u + \xi) \in \mathbb{Z}vk \oplus \mathbb{Z}v(u + \xi)
\end{aligned}$$

pois $N(u + \xi) = kc$, com $c \in \mathbb{Z}$, por hipótese.

Quanto à unicidade de k e v, sejam $k', v' \in \mathbb{Z}$ positivos e $u' \in \mathbb{Z}$ tais que

$$I = \mathbb{Z}v'k' \oplus \mathbb{Z}v'(u' + \xi).$$

Existem $a, b \in \mathbb{Z}$, únicos, tais que $v'(u'+\xi) = akv+bv(u+\xi)$, pois $v'(u'+\xi) \in I$. Comparando os coeficientes de ξ obtemos $v' = bv$. Dessa forma, $v|v'$. Invertendo as posições dos elementos v', k', u' com v, k, u, obteremos que $v'|v$. Logo $v' = v$. Por outro lado,

$$kv\mathbb{Z} = I \cap \mathbb{Z} = k'v'\mathbb{Z}.$$

Como k, v, k' e v' são positivos, $kv = k'v'$ e, pela igualdade anterior, $k' = k$, como queríamos.

■

Conforme a notação que introduzimos nesse capítulo, o ideal I é representado por $(vk, v(u+\xi))$

Proposição 4.1.2. (a) *Sejam $(vk, v(u + \xi))$ um ideal não nulo de $O(m)$ e u' um inteiro tal que $u' \equiv u \ (mod\ k)$. Então, $(vk, v(u + \xi)) = (vk, v(u' + \xi))$.*

(b) *Dado o ideal $I = (vk, v(u + \xi))$, com $k|N(u + \xi)$, sempre é possível escolher um único u tal que $0 \leq u < k$.*

Demonstração.

(a) Lembra-se que

$$f(X) = X^2 + T(\xi)X + N(\xi).$$

Seja $u = u' + kq$, com $q \in \mathbb{Z}$, então

$$\begin{aligned} f(u) &= u^2 + T(\xi)u + N(\xi) = (u' + kq)^2 + T(\xi)(u' + kq) + N(\xi) \\ &= (u')^2 + 2u'kq + k^2q^2 + T(\xi)u' + T(\xi)kq + N(\xi) \\ &= f(u') + 2u'kq + k^2q^2 + T(\xi)kq \end{aligned}$$

Como $2u'kq + k^2q^2 + T(\xi)kq \equiv 0(mod\ k)$, segue que $f(u) \equiv f(u')(mod\ k)$. Logo $k|N(u' + \xi)$ também e assim $(vk, v(u' + \xi))$ é ideal de $O(m)$. Verifiquemos a igualdade dos ideais. Seja $u = u' + kq$. Então

$$v(u + \xi) = vkq + v(u' + \xi) \in (vk, v(u' + \xi))$$

e assim

$$(vk, v(u + \xi)) \subseteq (vk, v(u' + \xi)).$$

Igualmente $u' = u + k(-q)$ e assim

$$v(u' + \xi) = vk(-q) + v(u + \xi) \in (vk, v(u + \xi))$$

e também $(vk, v(u' + \xi)) \subseteq (vk, v(u + \xi))$, resultando a igualdade.

(b) Consequência imediata de (a).

■

4.2 A Norma de um Ideal

Veremos agora que, assim como $\mathbb{Z}$, $O(m)$ tem um número finito de classes de congruência módulo um ideal. Recordemos que, como usualmente, $\mathbb{Z}_n$ representa o conjunto das classes de equivalência de $\mathbb{Z}$ módulo n, ou ainda, o anel quociente de $\mathbb{Z}$ pelo ideal $n\mathbb{Z}$.

Proposição 4.2.1. *Para todo ideal $I = (vk, v(u+\xi))$ o anel quociente $O(m)/I$ é finito com v^2k elementos, com v e k positivos.*

Demonstração. Primeiramente, observe que $O(m) = \mathbb{Z} \oplus \mathbb{Z}(u+\xi)$, pois dado $x = a+b\xi \in O(m)$, podemos escrever

$$x = a + b\xi = (a - bu) + b(u + \xi) \in \mathbb{Z} \oplus \mathbb{Z}(u + \xi)$$

Defina

$$\varphi : O(m) \longrightarrow \mathbb{Z}_{vk} \times \mathbb{Z}_v$$

por

$$\varphi(a + b(u + \xi)) = (\overline{a}, \overline{b}).$$

É fácil verificar que φ é um homomorfismo sobrejetor de grupos aditivos. Dado $x = a+b(u+\xi) \in O(m)$, temos

$$\begin{aligned} x \in Ker\varphi &\Leftrightarrow (\overline{a}, \overline{b}) = (\overline{0}, \overline{0}) \in \mathbb{Z}_{vk} \times \mathbb{Z}_v \\ &\Leftrightarrow a = vkq \text{ e } b = vq', \text{ com } q, q' \in \mathbb{Z} \\ &\Leftrightarrow x = vkq + q'v(u + \xi) \in I. \end{aligned}$$

Logo, $Ker(\varphi) = I$. Segue do Teorema Fundamental dos Homomorfismos para grupos ([10, Teorema 3.22],) que

$$\frac{O(m)}{I} \simeq \mathbb{Z}_{vk} \times \mathbb{Z}_v.$$

Como $\mathbb{Z}_{vk} \times \mathbb{Z}_v$ é finito, segue que $O(m)/I$ é finito, com cardinalidade igual a $\mathbb{Z}_{vk} \times \mathbb{Z}_v$, que é $vk.v = v^2k$.

■

Definição 4.2.2. *Dado um ideal não nulo $I = (vk, v(u+\xi))$ de $O(m)$, chama-se de norma de I o número v^2k que é igual à cardinalidade do anel quociente $O(m)/I$.*

Denotaremos a norma de I por $N(I)$. Nos próximos resultados verificaremos que $N(I)$ tem propriedades bem semelhantes à norma de um elemento definida na Seção 1.1. Para isso vamos definir $\overline{I} = \{\overline{\alpha} | \alpha \in I\}$ como o *conjugado do ideal I*. Claramente $\overline{I} = (vk, v(u + \overline{\xi}))$, se $I = (vk, v(u+\xi))$. Além disso, é fácil ver que $N(I) = N(\overline{I})$.

Proposição 4.2.3. *Seja $I = (vk, v(u+\xi))$, com $0 \leq u < k$ e $k | N(u+\xi)$, um ideal não nulo de $O(m)$. Então $I\overline{I} = N(I)O(m)$.*

Demonstração. Seja $N(u+\xi) = kt$, com $t \in \mathbb{Z}$. Por definição temos que $N(I) = v^2k$. Sejam $x = vkq_1 + v(u+\xi)q_2$ e $\overline{y} = vkq_1{}' + v(u+\overline{\xi})q_2{}'$, com $q_1, q_2, q_1', q_2' \in \mathbb{Z}$. Então,

$$\begin{aligned} x\overline{y} &= (vkq_1 + v(u+\xi)q_2)(vkq_1{}' + v(u+\overline{\xi})q_2{}') \\ &= v^2k^2q_1q_1{}' + v^2kq_1(u+\overline{\xi})q_2{}' + v^2k(u+\xi)q_2q_1{}' + v^2(u+\xi)(u+\overline{\xi})q_2q_2' \\ &= v^2k^2q_1q_1{}' + v^2kq_1(u+\overline{\xi})q_2{}' + v^2k(u+\xi)q_2q_1{}' + v^2N(u+\xi)q_2q_2{}' \\ &= v^2k^2q_1q_1{}' + v^2kq_1(u+\xi)q_2{}' + v^2k(u+\xi)q_2q_1{}' + v^2ktq_2q_2{}' \\ &= v^2k(kq_1q_1{}' + (u+\xi)q_1q_2{}' + (u+\xi)q_2q_1{}' + tq_2q_2{}'). \end{aligned}$$

Assim, $I\overline{I} = vk^2J$, onde

$$J = k\mathbb{Z} + (u+\xi)\mathbb{Z} + (u+\overline{\xi})\mathbb{Z} + t\mathbb{Z} \tag{4.3}$$

é um ideal de $O(m)$. Vamos mostrar que $J = O(m)$.

Se $m \not\equiv 1(mod\ 4)$, então $\xi = \sqrt{m}$, $\overline{\xi} = -\sqrt{m}$ e $N(u+\xi) = u^2 - m = kt$. Seja $g = mdc(k, 2u, t)$ e suponhamos que existe primo p tal que $p|g$. Logo $p|k$ e $p|t$, e assim $p^2|N(u+\xi)$. Se p é ímpar, então $p|u$ e portanto $p^2|m$, contra hipótese de m ser livre de quadrados. Se $p = 2$, então $u^2 \equiv m(mod\ 4)$. Como $m \equiv 2(mod\ 4)$ ou $m \equiv 3(mod\ 4)$ temos um absurdo pois $u^2 \equiv 0$ ou $1\ (mod\ 4)$. Logo $g = 1$ e existem $x, y, z \in \mathbb{Z}$ tais que $1 = xk + 2uy + zt$. Por (4.3). Assim

$$1 = xk + y(u+\xi) + y(u+\overline{\xi}) + zt \in J$$

e $J = O(m)$, por [10] Capítulo 5 p. 376.

Se $m \equiv 1(mod\ 4)$, então $\xi = \dfrac{1+\sqrt{m}}{2}$, $\overline{\xi} = \dfrac{1-\sqrt{m}}{2}$ e

$$N(u+\xi) = u^2 + u + (1-m)/4 = [(2u+1)^2 - m]/4. \tag{4.4}$$

Assim, $4kt = (2u+1)^2 - m$. Seja agora $g = mdc(k, (2u+1), t)$ e suponha p primo tal que $p|g$. Logo, $p^2|4kt$ e $p^2|(2u+1)^2$. Segue de (4.4), $p^2|m$, o que é um absurdo. Portanto $g = 1$ e existem $x, y, z \in \mathbb{Z}$ tais que $1 = xk + y(2u+1) + zt$. Assim,

$$1 = xk + y(u+\xi) + y(u+\overline{\xi}) + zt \in J$$

e novamente $J = O(m)$. ∎

Vamos agora mostrar que a norma de ideais tem propriedades semelhantes às da norma de números.

Teorema 4.2.4. *Sejam I e J ideais não nulos de $O(m)$ e $\alpha \in O(m)$, $\alpha \neq 0$.*

(a) *Se $\alpha \in \mathbb{Z}$, então $N(\alpha O(m)) = \alpha^2 = N(\alpha)$.*

(b) $N(IJ) = N(I)N(J)$.

(c) $N(\alpha O(m)) = ||N(\alpha)||$.

(d) *Se $I \subseteq J$ e $N(I) = N(J)$, então $I = J$.*

Demonstração.

(a) Observe que $\alpha O(m) = \alpha\mathbb{Z} \oplus \alpha\xi\mathbb{Z}$. Pela demonstração da Proposição 4.2.1 temos que

$$\varphi : O(m) \longrightarrow \mathbb{Z}_\alpha \times \mathbb{Z}_\alpha$$

definida por $\varphi(a+b\xi) = (\overline{a}, \overline{b})$ é um homomorfismo sobrejetor de grupos com $Ker\varphi = \alpha O(m)$. Logo, $\dfrac{O(m)}{\alpha O(m)} \simeq \mathbb{Z}_\alpha \times \mathbb{Z}_\alpha$ e portanto $N(\alpha O(m)) = \alpha^2$.

(b) Pela Proposição 4.2.3 temos $IJ\overline{IJ} = N(IJ)O(m)$ e assim, pelo item (a),

$$N(IJ\overline{IJ}) = N(IJ)^2. \tag{4.5}$$

Por outro lado, $\overline{IJ} = \overline{I}\ \overline{J}$ e assim

$$IJ\overline{IJ} = I\overline{I}J\overline{J} = N(I)O(m)N(J)O(m) = N(I)N(J)O(m).$$

Resulta então que

$$lN(IJ\overline{IJ}) = (N(I)N(J))^2. \tag{4.6}$$

Como normas de ideais são números positivos, segue de (4.5) e (4.6) que $N(IJ) = N(I)N(J)$.

(c) Tomando $I = \alpha O(m)$ e $J = \overline{\alpha}O(m)$ no item anterior e usando (a), obtemos

$$\begin{aligned} N(\alpha)^2 &= N(\alpha\overline{\alpha}O(m)) = N(IJ) \\ &= N(I)N(J) = N(\alpha O(m))N(\overline{\alpha}O(m)) \\ &= N(\alpha O(m))^2 \end{aligned}$$

pois $N(I) = N(\overline{I})$. Assim, como no item (b), temos que $N(\alpha O(m)) = ||N(\alpha)||$.

(d) Sejam $I = (kv, v(u+\xi))$ e $J = (k_1v_1, v_1(u_1+\xi))$, como no Teorema 4.1.1. Como $N(I) = N(J)$, temos por definição

$$kv^2 = k_1v_1^2. \tag{4.7}$$

Por outro lado, $I \cap \mathbb{Z} \subseteq J \cap \mathbb{Z}$ implica que k_1v_1 divide kv. Seja $kv = k_1v_1t$ para algum $t \in \mathbb{Z}$. Multiplicando essa igualdade por v e levando em conta (4.7), obtemos $k_1v_1^2 = vk_1v_1t$. Cancelando os fatores comuns, chegamos em $v_1 = vt$, ou seja, v divide v_1.

Consideramos agora que $v(u+\xi) \in J$. Logo, existem $a, b \in \mathbb{Z}$ tais que

$$v(u+\xi) = ak_1v_1 + bv_1(u_1+\xi).$$

Comparando os coeficiente de ξ vemos que $v = bv_1$, ou seja, v_1 divide v. Logo temos que $v = v_1$, e por (4.7) que $k = k_1$. Finalmente observamos que

$$v(u_1+\xi) - v(u+\xi) = v(u_1-u) \in J \cap \mathbb{Z} = vk\mathbb{Z}.$$

Dessa forma, $u_1 \equiv u\ (mod\ k)$ e, pela Proposição 4.1.2, concluímos que $I = J$.

■

Apêndice A

Apresentamos abaixo o código desenvolvido no Python usado para encontrar as unidades fundamental do anel $O(m)$, seguindo os passos da Observação 3.3.8:

```
def fu(c,m,b):
    return c+m*b**2
def fl(c,m,b):
    return -c+m*b**2
m = int(input("Digite o valor de m"))
b = 1
if m % 4 == 1:
    c = 4
else:
    c = 1
while True:
    al = fl(c,m,b)**(0.5)
    au = fu(c,m,b)**(0.5)
    if al.is_integer():
        print(f'-{c}+{m}*{b}^2 é um quadrado perfeito e o valor de b é {b}')
        if m % 4 != 1:
            print(f'{al} + {b} * sqrt{m}')
        else:
            print(f'{al}/2 + {b}/2 * sqrt{m}')
    if au.is_integer():
        print(f'teste {c}+{m}*{b}^2 é um quadrado perfeito e o valor de b é {b}')
        if m % 4 != 1:
            print(f'{au}+{b} * sqrt{m}')
        else:
            print(f'{au}/2+{b}/2 * sqrt{m}')
    if al.is_integer() or au.is_integer():
            break
    else:
        b += 1
```

Referências Bibliográficas

[1] H. Chatland, On the eucllidian algorithm in quadratic number fields, Amer. Math. Soc. 55 (1949) 948–953.

[2] E. Barnes, H. Swinnerton-Dyer, The inhomogeneous minima of binary quadratic forms (i), Acta Math. 87 (1952) 259–323.

[3] P. Samuel, About euclidean rings, Journal of Algebra 19 (1971) 282–301.

[4] J. F. S. Andrade, Tópicos especiais em álgebra, Sociedade Brasileira de Matemática, 2013.

[5] J. F. Andrade, Anéis quadráticos euclidianos, Revista Matemática Universitária (RMU) nº48 e 49 (2012).

[6] G. d. F. Djairo, Números Irracionais e Transcendentes, SBM, 2011.

[7] O. Endler, Teoria dos números algébricos, Vol. 15, Instituto de Matemática Pura e Aplicada, CNPq, 2014.

[8] A. J. Engler, Inteiros quadráticos eo grupo de classes: 23. Colóquio Brasileiro de Matemática, Instituto de Matemática Pura e Aplicada (IMPA), 2001.

[9] C. P. Milies, S. P. Coelho, Números: Uma introdução à Matemática, Universidade de São Paulo, 2013.

[10] V. L. Vieira, Álgebra Abstrata para Licenciatura, EDUEPB, 2015.

[11] J. B. Fraleigh, A first course in abstract algebra, Pearson Education India, 2003.

[12] H. Denvenport, Indefinite binary quadratic forms and euclid's algorithm in real quadratic fields, Proc. London Math. Soc. 53 (1951) 65–82.