VIVIANE MARIA BEUTER

O ANEL DE INTEIROS QUADRÁTICOS

Florianópolis
2008

Universidade Federal de Santa Catarina
Centro de Ciências Físicas e Matemáticas
Departamento de Matemática

O ANEL DE INTEIROS QUADRÁTICOS

Trabalho de Conclusão de Curso
apresentado ao Curso de Matemática
Habilitação Bacharelado
Departamento de Matemática
Centro de Ciências Físicas e Matemáticas
Universidade Federal de Santa Catarina

Viviane Maria Beuter

Orientador
Dr. Oscar Ricardo Janesch

Florianópolis, fevereiro de 2008.

Esta monografia foi julgada adequada como **TRABALHO DE CONCLUSÃO DE CURSO** no curso de Matemática - Habilitação Bacharelado em Matemática e Computação Científica, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria n^o. $58/CCM/07$.

Prof^a. Carmen Suzane Comitre Gimenez
Professora responsável pela disciplina

Banca Examinadora:

Prof. Dr. Oscar Ricardo Janesch (UFSC-Orientador)

Prof. Dr. Eliezer Batista (UFSC)

Prof. Dr. Danilo Royer (UFSC)

Agradecimentos

À Deus, pela saúde e por permitir a realização de mais um sonho.

À UFSC, por propiciar os meios para a realização deste trabalho.

Ao meu orientador, Prof. Dr. Oscar Ricardo Janesch, pela forma profissional pela qual conduziu seu trabalho de orientador.

À minha mãe e ao meu irmão/pai, pela força, perseverança, união e pelo imenso amor.

À toda a minha família, em especial aos meus padrinhos, pelo apoio e incentivo.

Aos meus mais que colegas, grandes amigos que conquistei ao longo da graduação:
Fabi, Rafa, Jonatan, Ismael, Gil, Rick, Paôla, Tiago, Dehia, Né, Pati, Fábio, Rô, Cintia, Elia e demais amigos da matemática, o meu muito obrigada pela compreensão, ajuda e amizade.

Sumário

Introdução

Entre os anos de 1808 e 1825, o matemático alemão Carl F. Gauss, investigava questões relacionadas à reciprocidade cúbica e à reciprocidade biquadrática, quando percebeu que essa investigação se tornava mais simples trabalhando sobre $\mathbb{Z}[i]$, o anel dos inteiros gaussianos, do que em $\mathbb{Z}$, o conjunto dos números inteiros. O conjunto $\mathbb{Z}[i]$ é formado pelos números complexos da forma a + bi, onde a e b são números inteiros e $i = \sqrt{-1}$.

Gauss estendeu a idéia de número inteiro quando definiu o conjunto $\mathbb{Z}[i]$, pois descobriu que muito da antiga Teoria de Euclides sobre fatoração de inteiros, poderia ser transportada para $\mathbb{Z}[i]$ com conseqüências importantes para a Teoria dos Números. Ele desenvolveu uma Teoria de Fatoração em Primos para esses números complexos e demonstrou que essa decomposição em primos é única, como acontece com o conjunto dos números inteiros. O uso que Gauss fez desse novo tipo de número foi de fundamental importância na demonstração do Último Teorema de Fermat.

Os inteiros de Gauss são exemplos de um tipo particular de número complexo, ou seja, números complexos que são soluções de uma equação polinomial

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

onde todos os coeficientes são números inteiros. Esses números complexos que são raízes de uma equação polinomial com coeficientes inteiros são chamados de números inteiros algébricos. Por exemplo, a unidade imaginária, i, é um inteiro algébrico, pois satisfaz a equação $x^2 + 1 = 0$. Também a raiz quadrada $\sqrt{2}$ é um inteiro algébrico, pois satisfaz a equação $x^2 - 2 = 0$. Observe que os números i e $\sqrt{2}$ são exemplos de inteiros algébricos e não são números inteiros.

A generalização da noção de número inteiro para número inteiro algébrico dá exemplos especiais de desenvolvimentos muito mais profundos que chamamos de Teoria dos Números Algébricos.

Outra motivação para o estudo da aritmética de números algébricos, origina-se da Teoria das Equações Diofantinas. Por exemplo, uma forma quadrática definida sobre um anel A é um polinômio homogêneo em duas variáveis e de grau 2, tal que os coeficientes são elementos de A, isto é, polinômios da forma $f(x, y) = ax^2 + bxy + cy^2$ onde a, b, c pertencem ao anel A. Se

tomarmos a forma quadrática sobre o anel dos números inteiros

$$f(x, y) = x^2 - my^2,$$

onde m é um número inteiro e $\sqrt{m}$ não é um número inteiro, essa pode ser escrita na forma

$$f(x, y) = x^2 - my^2 = (x - \sqrt{m}y)(x + \sqrt{m}y).$$

Portanto, a questão sobre a possibilidade da representação de inteiros r por $r = a^2 - mb^2 = f(a, b)$ onde a e b são números inteiros, é reformulada como uma questão de fatoração de números algébricos do anel $\mathbb{Z}[\sqrt{m}]$, isto é, números da forma $a + b\sqrt{m}$. Essas motivações deixam evidente a importância dos anéis $\mathbb{Z}[\sqrt{m}]$ e $\mathbb{Z}[i]$.

Em boa parte desse trabalho falamos de números primos, irredutíveis e principalmente sobre anéis fatoriais, euclidiano e principais. Para uma melhor compreensão desse conteúdo foi elaborado um apêndice onde abordamos conceitos elementares sobre esse assunto, para um anel de integridade qualquer. O leitor que não estiver familiarizado, pode ler o apêndice antes.

Nos dois primeiros capítulos apresentamos algumas noções de teoria dos números algébricos, para com isso definir um corpo quadrático e um anel de interios quadráticos. No capítulo 1 definimos e caracterizamos um corpo quadrático $\mathbb{Q}[\sqrt{m}]$, e mostramos as propriedades da norma e traço desse corpo. Já no segundo capítulo, definimos e caracterizamos o anel dos inteiros quadráticos $\mathcal{O}(m)$ com relação ao inteiro m, um dos objetivos desse trabalho. Nesse mesmo capítulo damos um destaque ao exemplo mais importante de um anel de inteiros algébricos, o anel dos inteiros de Gauss. A idéia é descrever os inversíveis (unidades) desse anel, e principalmente mostrar que é euclidiano, e portanto principal e fatorial. Nos dois próximos capítulos, induzidos pelo trabalho feito sobre os interios de Gauss, o objetivo é fazer um estudo geral dos anéis de inteiros quadráticos, descrever as unidades de cada um, e verificar (quando possível) quais anéis são fatoriais. Como todo anel euclidiano é fatorial, mostramos para quais valores de m os anéis $\mathcal{O}(m)$ são euclidianos, em relação a norma absoluta. Porém, para ser um anel fatorial é suficiente ser euclidiano, mas não necessário. Então no capítulo 5 é feito um estudo sobre os ideais de $\mathcal{O}(m)$, e mostrado que num anel de inteiros algébricos $\mathcal{O}(m)$ é fatorial se e somente se é principal.

Para verificar quando um anel de interios quadráticos é principal, é necessário um estudo aprofundado de grupo de classes, que é um trabalho complexo e extenso. Isso não será feito neste trabalho.

1 Corpos Quadráticos

Um dos exemplos mais simples de corpos de Números Algébricos, são os corpos quadráticos. Veremos que um corpo quadrático é uma extensão finita de $\mathbb{Q}$, de grau 2, que fica determinado por um elemento primitivo $\sqrt{m}$, onde m é um número inteiro livre de quadrados.

1.1 Noções básicas sobre números algébricos

Nesta seção consideramos L um corpo, tal que $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$, e consideramos L como um $\mathbb{Q}$ - espaço vetorial. Dizemos que L é uma *extensão* de $\mathbb{Q}$, e que L é uma *extensão finita* de grau $[L : \mathbb{Q}] = n$, quando uma (e logo toda) base do $\mathbb{Q}$ - espaço vetorial L tiver n elementos.

Definição 1.1.

(i) Um elemento $\alpha \in L \subseteq \mathbb{C}$ é um número algébrico sobre $\mathbb{Q}$ se existe um polinômio mônico $p(x) \in \mathbb{Q}[x]$ tal que $p(\alpha) = 0$.

(ii) Uma extensão algébrica de $\mathbb{Q}$ é um subcorpo L de $\mathbb{C}$ tal que todo elemento de L é algébrico sobre $\mathbb{Q}$

(iii) Um subcorpo L de $\mathbb{C}$ será chamado corpo de números algébricos se for uma extensão finita de $\mathbb{Q}$.

Observação 1.1. Note que toda extensão finita de $\mathbb{Q}$ é extensão algébrica. De fato, sejam L subcorpo de $\mathbb{C}$ tal que $[L : \mathbb{Q}] = m < \infty$ e $\alpha \in L$. Desde que $\mathbb{Q}[\alpha]$ é $\mathbb{Q}$ - subespaço vetorial do $\mathbb{Q}$ - espaço vetorial L, temos que $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n \leq m$. Como $\{1, \alpha, \cdots, \alpha^n\}$ é LD, existem $a_0, a_1, \cdots, a_n \in \mathbb{Q}$, não todos nulos, tais que $0 = a_0 + a_1\alpha + \cdots a_n\alpha^n$. Tome

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}[x] \setminus \{0\}.$$

Como $f(\alpha) = 0$, concluímos que α é algébrico sobre $\mathbb{Q}$

O teorema abaixo assegura, em particular, que todo corpo de números algébricos pode ser obtido pela adjunção de um único elemento. Aqui lembramos que se $K \subseteq L$ é uma extensão de

corpos e $u \in L$, então por definição,

$$K[u] = \{f(u); f(x) \in \ K[x]\}.$$

Teorema 1.1 (Teorema do Elemento Primitivo). *Seja $L \supseteq K \supseteq \mathbb{Q}$ tal que $[L : K] < \infty$. Então, $\exists\, u \in L$ tal que $L = K[u]$.*

Demonstração: Ver ([4], página 102).

Seja L um corpo de números algébricos, pelo Teorema do Elemento Primitivo tem-se $L = \mathbb{Q}[u]$. Desde que $[L : \mathbb{Q}] < \infty$, segue da Observação 1.1 que L é extensão algébrica de $\mathbb{Q}$. Assim todo elemento de L é algébrico sobre $\mathbb{Q}$. Em particular u é algébrico sobre $\mathbb{Q}$.

Seja $p(x)$ um polinômio mônico não nulo em $\mathbb{Q}[x]$ de menor grau tal que $p(u) = 0$. Pela minimalidade do grau, segue que $p(x)$ é o único polinômio mônico irredutível em $\mathbb{Q}[x]$ tal que $p(u) = 0$. Chamamos $p(x)$ de *polinômio minimal* de u.

Lema 1.1. *Sejam L uma extensão de $\mathbb{Q}$ e $\alpha \in L$ algébrico sobre $\mathbb{Q}$. Então $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ é exatamente o grau do polinômio minimal de α sobre $\mathbb{Q}$.*

Demonstração: Sejam $p(x) \in \mathbb{Q}[x]$ o polinômio minimal de α e n o grau de $p(x)$. Vamos primeiro mostrar que para todo polinômio $f(x) \in \mathbb{Q}[x]$ não nulo, $f(\alpha)$ pode ser expresso de modo único na forma,

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

com $a_i \in \mathbb{Q}$. Pelo algoritmo da divisão, $f(x)$ pode ser escrito como,

$$f(x) = q(x)p(x) + a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

onde $q(x) \in \mathbb{Q}[x]$. Então,

$$f(\alpha) = q(\alpha)p(\alpha) + a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

pois $p(\alpha) = 0$.

Para mostrar a unicidade da expressão temos que, se

$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1},$$

com a_i, $b_i \in \mathbb{Q}\ \ \forall i \in \{1, \cdots, n-1\}$ segue que o polinômio $h(x) \in \mathbb{Q}[x]$, com

$$h(x) = (a_0 - b_0) + (a_1 - b_1)x + \cdots + (a_{n-1} - b_{n-1})x^{n-1}$$

é tal que $h(\alpha) = 0$. O grau de $h(x)$ é menor que o grau de $p(x)$. Pela minimalidade do grau de $p(x)$ temos que $h(x) \equiv 0$. Então $a_i = b_i\ \ \forall\, i \in \{1, \cdots, n-1\}$.

Com isso, $\mathbb{Q}[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\,;\ \ a_i \in \mathbb{Q}\}$.

Vamos mostrar agora que $\beta = \{1, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{Q}[\alpha]$.
É imediato que β gera $\mathbb{Q}[\alpha]$. Falta verificar que β é L.I. Sejam $b_1, \cdots, b_{n-1} \in \mathbb{Q}$,

$$\sum_{i=0}^{n-1} b_i\alpha^i = 0 = \sum_{i=0}^{n-1} 0\alpha^i$$

Pela unicidade, $b_i = 0\ \ \forall\ i \in \{1, \cdots, n-1\}$.
Como $\beta = \{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{Q}[\alpha]$ sobre $\mathbb{Q}$, então $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ ■

Observação 1.2. Uma vez que todo elemento α de um corpo de números algébricos L é um número algébrico, segue que L é uma extensão algébrica de $\mathbb{Q}$. Porém a recíproca não é verdadeira.

De fato, seja $L = \{\alpha \in \mathbb{R}; \alpha \text{ algébrico sobre } \mathbb{Q}\}$. Vamos verificar que L é um subcorpo de $\mathbb{R}$, e uma extensão algébrica infinita de $\mathbb{Q}$. Claramente o subconjunto L de $\mathbb{R}$ contém $\mathbb{Q}$. Para provarmos que L é um subcorpo de $\mathbb{R}$ é suficiente provarmos as seguintes propriedades:

- $\alpha, \beta \in L \Rightarrow \alpha - \beta \in L$
- $\alpha, \beta \in L \Rightarrow \alpha \cdot \beta \in L$
- $0 \neq \alpha \in L \Rightarrow \alpha^{-1} \in L$

Vamos mostrar simultaneamente os itens. Sejam α, $\beta \in L$. Sejam $K = \mathbb{Q}[\alpha]$ e $M = K[\beta]$. Como α é algébrico sobre $\mathbb{Q}$ segue que $[K : \mathbb{Q}] < \infty$. Agora sendo β algébrico sobre $\mathbb{Q}$, β também é algébrico sobre K e daí segue que $[M : K] < \infty$. Temos que,

$$[M : \mathbb{Q}] = [M : K][K : \mathbb{Q}] < \infty.$$

Logo, M é uma extensão finita de $\mathbb{Q}$, e então M é uma extensão algébrica. Agora o resultado sai imediatamente, pois $\alpha \pm \beta \in M$, $\alpha \cdot \beta \in M$ e $\dfrac{1}{\alpha} \in M$ se $\alpha \neq 0$. Portanto, $\alpha - \beta, \alpha \cdot \beta$ e $\alpha^{-1} \in L$ é uma extensão algébrica sobre $\mathbb{Q}$.

Agora se $\alpha_i = \sqrt[2^i]{2}$ e $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}[\alpha_1]$, $\cdots$, $K_i = K_{i-1}[\alpha_i]$ temos que

$$M = \bigcup_{i=0}^{\infty} K_i$$

é uma extensão algébrica infinita de $\mathbb{Q}$ e $M \subseteq L$.

1.2 Corpos quadráticos

Antes de definir um corpo quadráticos e caracterizá-lo, vamos definir um elemento inteiro livre de quadrados e ver alguns exemplos.

Definição 1.2. *Dizemos que $m \in \mathbb{Z}$, $m \neq 1$, é livre de quadrados quando o único quadrado que divide m é 1. Isto é, $x^2 \mid m$ implica que $x^2 = 1$.*

Exemplo 1.1.

(a) $m = -1$ é livre de quadrados.

(b) Se $m \in \mathbb{Z}$, $m \neq \pm 1$. Então m é livre de quadrados se, e somente se $-m$ é livre de quadrados. De fato, $x^2 \mid (-m) \Rightarrow x^2 \mid m \Rightarrow x^2 = 1$, pois m é livre de quadrados. A volta é análoga.

(c) Todo número primo p é livre de quadrados.
Suponha que $x^2 \mid p$, então $x \mid p$, logo $x = \pm 1$ ou $x = \pm p$.

- $x = \pm p \Rightarrow p^2 \mid p \Rightarrow p^2 \cdot y = p$, para algum $y \in \mathbb{Z} \Rightarrow p \cdot y = 1 \Rightarrow p$ é inversível. Absurdo!
- $x = \pm 1 \Rightarrow x^2 = 1 \Rightarrow p$ é livre de quadrados.

(d) Se $m \in \mathbb{Z}$ é livre de quadrados, então $\sqrt{m} \notin \mathbb{Q}$.
Suponha que $\sqrt{m} \in \mathbb{Q}$, então $\sqrt{m} = \dfrac{p}{q}$ com $mdc(p, q) = 1$, p, $q \in \mathbb{Z}$.
Temos $mq^2 = p^2 \Rightarrow p \mid m \Rightarrow m = pt$, para algum $t \in \mathbb{Z}$.
Da equação $mq^2 = p^2$ obtemos $ptq^2 = p^2 \Rightarrow tq = p \Rightarrow p \mid t \Rightarrow pu = t$, para algum $u \in \mathbb{Z}$.
Substituindo a última igualdade em $m = pt$, temos que $m = p^2u$ e então $p^2 \mid m$. Como m é livre de quadrados temos que $p^2 = 1$. Absurdo!

Vamos definir agora um corpo quadrático.

Definição 1.3. *Um corpo de números algébricos K é chamado de corpo quadrático quando o grau da extensão é 2 ($[K : \mathbb{Q}] = 2$).*

Proposição 1.1. *Um corpo quadrático K é da forma $\mathbb{Q}[\sqrt{m}]$, onde m é um número inteiro livre de quadrados.*

Demonstração: Por definição, um corpo quadrático K é um corpo de números algébricos de grau 2. Então existe $\alpha \in K$ tal que $K = \mathbb{Q}[\alpha]$, e $[K : \mathbb{Q}] = 2$. Logo, o grau do polinômio minimal de α é 2. Seja $p(x) = x^2 + bx + c \in \mathbb{Q}[x]$ o polinômio minimal de α. Resolvendo a equação quadrática $\alpha^2 + b\alpha + c = 0$, temos que $\alpha = \dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$. Desta maneira

$$K = \mathbb{Q}[\alpha] = \mathbb{Q}\left[\frac{-b \pm \sqrt{b^2 - 4c}}{2}\right] = \mathbb{Q}[\sqrt{b^2 - 4c}],$$

e observando que $b^2 - 4c$ é um número racional da forma $\frac{u}{v} = \frac{uv}{v^2}$, com $u, v \in \mathbb{Z}$ e primos entre si, temos que

$$\mathbb{Q}[\sqrt{b^2 - 4c}] = \mathbb{Q}[\sqrt{uv}].$$

Como $uv \in \mathbb{Z}$, podemos representar $uv = d^2m$, onde d e m são números inteiros, $d > 0$, $m \neq 1$ e m livre de quadrados. Assim,

$$K = \mathbb{Q}[\sqrt{uv}] = \mathbb{Q}[\sqrt{m}],$$

onde m é um inteiro livre de quadrados. ■

Observação 1.3. Seja $m \in \mathbb{Z}$, m livre de quadrados. Por definição, $\mathbb{Q}[\sqrt{m}] = \{f(\sqrt{m}); f(x) \in \mathbb{Q}[x]\}$. Logo $\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m};\ \ a, b \in \mathbb{Q}\}$.
De fato, seja $u = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$. Para $f(x) = a + bx \in \mathbb{Q}[x]$ temos que $f(\sqrt{m}) = u$. Logo $u \in \mathbb{Q}[\sqrt{m}]$. Reciprocamente, seja $u \in \mathbb{Q}[\sqrt{m}]$. Então existe $f(x) \in \mathbb{Q}[x]$ tal que $u = f(\sqrt{m})$. Temos que $g(x) = x^2 - m \in \mathbb{Q}[x]$ e $f(x) = (x^2 - m)q(x) + r(x)$, $r(x) = a + bx \in \mathbb{Q}[x]$. Assim $u = f(\sqrt{m}) = r(\sqrt{m}) = a + b\sqrt{m}$.

Sejam $\alpha = a + b\sqrt{m}$ e $\beta = c + d\sqrt{m}$ elementos de $\mathbb{Q}[\sqrt{m}]$. As operações de *adição* e *multiplição* em $\mathbb{Q}[\sqrt{m}]$ ficam definidas respectivamente por:

$$\alpha + \beta = (a + b\sqrt{m}) + (c + d\sqrt{m}) = (a + c) + (b + d)\sqrt{m}$$

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

Num corpo quadrático $\mathbb{Q}[\sqrt{m}]$,

$$a + b\sqrt{m} = c + d\sqrt{m}, \text{ se e somente se } a = c \text{ e } b = d.$$

De fato, seja $a + b\sqrt{m} = c + d\sqrt{m}$, implica que $a - c = (d - b)\sqrt{m}$. Suponha $d \neq b$. Então $\sqrt{m} = \frac{a - c}{d - b} \in \mathbb{Q}$. Absurdo!

Observação 1.4. Como um corpo quadrático $\mathbb{Q}[\sqrt{m}]$ é uma extensão de grau 2 de $\mathbb{Q}$, temos que $\mathbb{Q}[\sqrt{m}]$ tem uma base com 2 vetores. Segue da Observação 1.3 que

$$\mathbb{Q}[\sqrt{m}] = \{a + b\sqrt{m};\ \ a, b \in \mathbb{Q}\} = \{a \cdot 1 + b \cdot \sqrt{m};\ \ a, b \in \mathbb{Q}\}.$$

Isso assegura que $\{1, \sqrt{m}\}$ é base do $\mathbb{Q}$ - espaço vetorial $\mathbb{Q}[\sqrt{m}]$.

Um corpo quadrático $\mathbb{Q}[\sqrt{m}]$ é dito *corpo quadrático real* se $m > 0$, isto é, $\mathbb{Q}[\sqrt{m}] \subseteq \mathbb{R}$ e se $m < 0$, $\mathbb{Q}[\sqrt{m}]$ é dito *corpo quadrático imaginário.*

Exemplo 1.2.

(a) Seja $m = 2$, temos que 2 é livre de quadrados, então o corpo $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}; a, b \in \mathbb{Q}\}$ é um corpo quadrático real.

(b) Um caso especial, e historicamente interessante é o *corpo dos números de Gauss* $\mathbb{Q}[i]$, onde $i = \sqrt{-1}$.

1.3 Norma e Traço

Teorema 1.2. *Seja $K = \mathbb{Q}[\alpha]$ um corpo de número algébrico de grau n. Então existem exatamente n monomorfismos $\sigma_i : K \to \mathbb{C}$. Os elementos $\sigma_i(\alpha) = \alpha_i$ são exatamente as raízes do polinômio minimal de α sobre $\mathbb{Q}$.*

Demonstração: Ver ([8], página 38).

Definição 1.4. *Seja K um corpo de números algébricos. Para $\beta \in K$ temos que $[\mathbb{Q}[\beta] : \mathbb{Q}] = n < \infty$, isto é, $\mathbb{Q}[\beta]$ é corpo de números algébricos. Se $\{\sigma_i;\ i \in \{1, \cdots, n\}\}$ é o conjunto de monomorfismos de $\mathbb{Q}[\beta]$ em $\mathbb{Q}$, definimos a Norma e o Traço de β, respectivamente por:*

$$\mathcal{N}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$$

$$\mathcal{T}_r(\beta) = \sum_{i=1}^{n} \sigma_i(\beta)$$

No caso em que $K = \mathbb{Q}[\sqrt{m}]$, onde m é livre de quadrados, os 2 monomorfismos de K em $\mathbb{C}$ são a identidade e a conjugação dados por $\sigma_1(\alpha) = \alpha$ e $\sigma_2(\alpha) = \overline{\alpha}$ respectivamente, onde $\alpha = a + b\sqrt{m}$ e $\overline{\alpha} = a - b\sqrt{m}$, com $a, b \in \mathbb{Q}$. Assim para $\alpha = a + b\sqrt{m}$;

$$\mathcal{N}(\alpha) = \alpha\overline{\alpha} = a^2 - mb^2$$

$$\mathcal{T}_r(\alpha) = \alpha + \overline{\alpha} = 2a.$$

Proposição 1.2. *Dados $\alpha, \beta \in \mathbb{Q}[\sqrt{m}]$ temos:*

(a) $\overline{\alpha} + \overline{\beta} = \overline{\alpha + \beta}$, $\overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$;

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

(c) $\mathcal{T}_r(\alpha + \beta) = \mathcal{T}_r(\alpha) + \mathcal{T}_r(\beta)$;

(d) $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$*;*

(e) $\mathcal{N}(\alpha) = 0$ *se e somente se* $\alpha = 0$*;*

(f) Se $\alpha \neq 0$, $\alpha^{-1} = \overline{\alpha}(\mathcal{N}(\alpha))^{-1}$.

Demonstração: Sejam $\alpha = a + b\sqrt{m}$ e $\beta = c + d\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$.

(a) $\overline{\alpha} + \overline{\beta} = a - b\sqrt{m} + c - d\sqrt{m} = a + c - (b + d)\sqrt{m} = \overline{\alpha + \beta}$;

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

(b) $\alpha = \overline{\alpha} \Leftrightarrow a + b\sqrt{m} = a - b\sqrt{m} \Leftrightarrow b = 0 \Leftrightarrow \alpha = a \in \mathbb{Q}$.

(c) $\mathcal{T}_r(\alpha + \beta) = \alpha + \beta + (\overline{\alpha + \beta}) = \alpha + \beta + \overline{\alpha} + \overline{\beta} = \alpha + \overline{\alpha} + \beta + \overline{\beta} = \mathcal{T}_r(\alpha) + \mathcal{T}_r(\beta)$.

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

(e) $\mathcal{N}(\alpha) = 0 \Leftrightarrow \alpha\overline{\alpha} = 0 \Leftrightarrow \alpha = 0$ ou $\overline{\alpha} = 0 \Leftrightarrow \alpha = 0$

(f) Se $\alpha \neq 0$, pelo item anterior $\mathcal{N}(\alpha) \neq 0$. Temos que:

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

■

A propriedade (c) diz que $\mathcal{T}_r : (\mathbb{Q}[\sqrt{m}], +) \to (\mathbb{Q}, +)$ é um homomorfismo de grupos. As propriedades (d) e (f) asseguram que $\mathcal{N} : (\mathbb{Q}[\sqrt{m}] \setminus \{0\}, \cdot) \to (\mathbb{Q} \setminus \{0\}, \cdot)$ é homomorfismo de grupos.

2 Inteiros Quadráticos

Pretendemos mostrar que todo corpo quadrático $\mathbb{Q}[\sqrt{m}]$ possui um subanel distinguido $\mathcal{O}(m)$, com corpo de frações igual a $\mathbb{Q}[\sqrt{m}]$. A descrição de $\mathcal{O}(m)$ depende de m, e em geral, não coincide com o anel $\mathbb{Z}[\sqrt{m}]$. Definiremos $\mathcal{O}(m)$ como o conjuntos dos elementos de $\mathbb{Q}[\sqrt{m}]$ que são "inteiros algébricos"sobre $\mathbb{Z}$.

2.1 Inteiros algébricos

Definição 2.1. *Sejam B um anel e A um subanel de B. Dizemos que o elemento $\alpha \in B$ é um inteiro sobre A se existe um polinômio mônico $f \in A[x]$ tal que $f(\alpha) = 0$. Isto é, existem $a_{n-1}, \cdots, a_1, a_0 \in A$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$.*

Denotamos o conjunto de todos os inteiros de B sobre A por $\mathcal{O}_B$:

$$\mathcal{O}_B = \{\alpha \in B; \alpha \text{ é inteiro sobre } A\}.$$

Definição 2.2. *No caso $B = \mathbb{C}$ e $A = \mathbb{Z}$, os números inteiros sobre $\mathbb{Z}$ são chamados inteiros algébricos. Isto é, um número complexo α é um inteiro algébrico se ele é raiz de um polinômio mônico com coeficientes em $\mathbb{Z}$.*

Teorema 2.1. *Sejam B um anel, A um subanel de B e $\alpha \in B$. As seguintes propriedades são equivalentes:*

(i) α é inteiro sobre A;

(ii) o anel $A[\alpha]$ é um A-módulo finitamente gerado;

(iii) existe um subanel C de B tal que C é um A-módulo finitamente gerado que contém A e α.

Demonstração:

$(i) \Rightarrow (ii)$ Suponha que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ com $a_{n-1}, \cdots, a_1, a_0 \in A$. Devemos mostrar que $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é um sistema de geradores do A-módulo $A[\alpha]$. De fato, a

partir de $\alpha^n = -\left(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0\right)$ segue que $\alpha^n, \alpha^{n+1}, \alpha^{n+2}, \cdots$ são expressos como combinação linear de $1, \alpha, \cdots, \alpha^{n-1}$, com coeficientes em A.

$(ii) \Rightarrow (iii)$ Como $\alpha \in A[\alpha]$ e $A \subset A[\alpha]$, é suficiente tomar $C = A[\alpha]$

$(iii) \Rightarrow (i)$ Seja $C =< y_1, \cdots, y_n >$ um A-módulo finitamente gerado tal que $A \subseteq C \subseteq B$ e $\alpha \in C$. Então, C é da forma $C = Ay_1 + \cdots + Ay_n$. Como $\alpha \in C$ temos $\alpha y_i \in C$, para $i = 1, \cdots, n$. Assim, existem $a_{ij} \in A$ com $1 \leq i, j \leq n$, de modo que:

$$\begin{cases} \alpha y_1 &= a_{11}y_1 &+ \cdots &+ a_{1n}y_n \\ \alpha y_2 &= a_{21}y_1 &+ \cdots &+ a_{2n}y_n \\ \quad\vdots & & & \\ \alpha y_n &= a_{n1}y_1 &+ \cdots &+ a_{nn}y_n \end{cases}$$

Logo,

$$\begin{cases} (\alpha - a_{11})y_1 - a_{12}y_2 - \cdots - a_{1n}y_n &= 0 \\ -a_{21}y_1 + (\alpha - a_{22})y_2 - \cdots - a_{2n}y_n &= 0 \\ \vdots & \\ -a_{n1}y_1 - a_{n2}y_2 - \cdots + (\alpha - a_{nn})y_n &= 0 \end{cases}$$

Na forma matricial, temos

$$\begin{bmatrix} (\alpha - a_n) & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & (\alpha - a_{22}) & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & (\alpha - a_{nn}) \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Seja D o determinante da matriz dos coeficientes do sistema linear. Pela Regra de Crammer, temos que $Dy_j = 0$, para $j = 1, \cdots, n$. Como $1 \in C$, segue que $1 = \sum_{j=1}^{n} c_j y_j$ com $c_j \in A$. Assim, $D = D.1 = D\sum_{j=1}^{n} c_j y_j = \sum_{j=1}^{n} c_j D y_j = 0$. Observemos que $D = \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_0 = 0$, onde cada $b_i \in A$. Portanto α é inteiro sobre A. ■

Corolário 2.1. *Sejam $A \subseteq B$ anéis, e sejam $\alpha_1, \cdots, \alpha_n \in B$. Se α_1 é inteiro sobre A, α_2 é inteiro sobre $A[\alpha_1]$, ... e α_n é inteiro sobre $A[\alpha_1, \cdots, \alpha_{n-1}]$. Então $A[\alpha_1, \cdots, \alpha_n]$ é um A-módulo finitamente gerado.*

Demonstração: Mostraremos por indução finita sobre n. Para $n = 1$, o Teorema 2.1 assegura

que $A[\alpha_1]$ é um A-módulo finitamente gerado. Vamos assumir que $B = A[\alpha_1, \cdots, \alpha_{n-1}]$ é um A-módulo finitamente gerado. Então $B = \sum_{j=1}^{s} Ab_j$. O caso $n = 1$ implica que $A[\alpha_1, \cdots, \alpha_n] = B[\alpha_n]$ é um B-módulo finitamente gerado. Escrevemos $B[\alpha_n] = \sum_{k=1}^{t} Bc_k$. Então

$$A[\alpha_1, \cdots, \alpha_n] = \sum_{k=1}^{t} Bc_k = \sum_{k=1}^{t} \left(\sum_{j=1}^{s} Ab_j \right) c_k = \sum_{j,k} Ab_j c_k.$$

Então $(b_j c_k)$ com $1 \leq j \leq s$ e $1 \leq k \leq t$ é um conjunto de geradores de $A[\alpha_1, \cdots, \alpha]$ como um módulo sobre A. ■

Corolário 2.2. *Sejam $A \subseteq B$ anéis. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\alpha \pm \beta$, $\alpha\beta$ são inteiros de A.*

Demonstração: Sejam $\alpha, \beta \in B$ inteiros sobre A. Então, $\alpha \pm \beta$, $\alpha\beta \in A[\alpha, \beta]$. Pelo corolário 2.1 temos que $A[\alpha, \beta]$ é um A-módulo finitamente gerado. Pelo Teorema 2.1 segue que $\alpha \pm \beta$, $\alpha\beta$ são inteiros sobre A. ■

Corolário 2.3. *Sejam $A \subseteq B$ anéis. O conjunto $\mathcal{O}_B$ dos elementos de B que são inteiros sobre A é um subanel de B que contém A.*

Demonstração: Pelo corolário 2.2, o conjunto $\mathcal{O}_B$ é um subanel de B. Temos que $A \subseteq \mathcal{O}_B$, pois, se $a \in A$, a é raiz do polinômio mônico $p(x) = x - a$ com coeficientes em A. ■

Seja A um domínio e B o corpo de frações de A. Dizemos que A é um anel *integralmente fechado* se $A = \mathcal{O}_B$.

Seja $K = \mathbb{Q}[u]$ um corpo de números algébricos e $\mathcal{O}_K$ o conjunto de todos os inteiros algébricos de K. O anel $\mathcal{O}_K$ é dito *anel de inteiros algébricos* de K.

Como $\mathcal{O}_K \subseteq \mathbb{C}$ é claro que $(\mathcal{O}_K, +)$ é um grupo abeliano, logo um $\mathbb{Z}$ - módulo.

Teorema 2.2. *Sejam K um corpo de números algébricos e $\mathcal{O}_K$ o anel de inteiros algébricos de K. Então $\mathcal{O}_K$ é um $\mathbb{Z}$ - módulo de posto finito. (denotamos posto de $\mathcal{O}_K$ por $\rho(\mathcal{O}_K)$) e $\rho(\mathcal{O}_K) = [K : \mathbb{Q}]$*

Demonstração: Ver ([7], página 40).

Definição 2.3. *Seja $\mathcal{O}_K$ o anel de inteiros de um corpo de números algébricos K. Uma $\mathbb{Z}$ - base de $\mathcal{O}_K$ é dita uma base integral.*

Observação 2.1. Desde que o $\rho(\mathcal{O}_K)$ é igual a $[K:\mathbb{Q}]$, toda base integral é uma $\mathbb{Q}$ - base para K. Isso segue do fato de que um conjunto $A \subseteq \mathbb{C}$ é $\mathbb{Z}$-linearmente independente se, e somente se, é $\mathbb{Q}$-linearmente independente.

2.2 O anel de inteiros quadráticos

Chegamos ao objetivo principal desse trabalho que é identificar o conjunto de todos os inteiros algébricos de $\mathbb{Q}[\sqrt{m}]$, que entretanto nem sempre é da forma $\mathbb{Z}[\sqrt{m}]$. Também vamos estudar algumas propriedades desses anéis de inteiros algébricos.

Definição 2.4. *Os inteiros algébricos de corpos quadráticos são chamados inteiros quadráticos.*

Denotaremos por $\mathcal{O}(m)$ o conjunto de todos os inteiros quadráticos de $\mathbb{Q}[\sqrt{m}]$.

Pelo Corolário 2.3, se $A \subseteq B$ é extensão de anéis, então $\mathcal{O}_B = \{\alpha \in B; \alpha \text{ é inteiro sobre } A\}$ é subanel de B. Portanto, $\mathcal{O}(m)$ é subanel de $\mathbb{Q}[\sqrt{m}]$.

Ao subanel $\mathcal{O}(m)$ chamamos de *Anel de inteiros quadráticos.*

Observação 2.2. Note que $\mathcal{O}(m)$ é um anel de integridade (domínio), uma vez que a comutatividade e a inexistência de divisores de zero é hereditário de $\mathbb{Q}[\sqrt{m}]$, e que 1 é raiz do polinômio mônico $p(x) = x - 1 \in \mathbb{Z}$.

Vamos mostrar agora que um elemento $\alpha \in \mathbb{Q}[\sqrt{m}]$ é um inteiro quadrático se e somente se $\mathcal{T}_r(\alpha)$ e $\mathcal{N}(\alpha)$ são números inteiros $\mathbb{Z}$. Para isso, precisamos de alguns resultados.

Proposição 2.1. *Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$. Então α é raiz do seguinte polinômio com coeficientes racionais*

$$f_\alpha(x) = x^2 - \mathcal{T}_r(\alpha)x + \mathcal{N}(\alpha)$$

Demonstração: Basta ver que $f_\alpha(x) = (x-\alpha)(x-\bar{\alpha})$. De fato,

$$f_\alpha(x) = (x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha} = x^2 - \mathcal{T}_r(\alpha)x + \mathcal{N}(\alpha)$$

■

O próximo teorema mostra que $\mathbb{Z}$ é um anel integralmente fechado.

Teorema 2.3. *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: Sejam $\alpha = \dfrac{a}{b} \in \mathbb{Q}$, $b \geq 1$, $mdc(a,b) = 1$ e

$$g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$$

tal que $g(\alpha) = 0$. Então

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

nos leva a conclusão de que b divide a^n. Segue que b divide a. Como a e b são primos entre si, resulta $b = 1$ e $\alpha \in \mathbb{Z}$. ■

Observação 2.3. Seja $m \neq -1$ um inteiro livre de quadrados. O elemento $\sqrt{m}$ é uma raiz do polinômio irredutível $x^2 - m$. O conjugado de $\sqrt{m}$ é $-\sqrt{m}$, ou seja, existe um automorfismo $\sigma : \mathbb{Q}[\sqrt{m}] \to \mathbb{Q}[\sqrt{m}]$, tal que $\sigma(a + b\sqrt{m}) = a - b\sqrt{m}$.

Além disso, se $\alpha \in \mathcal{O}(m)$ então $\sigma(\alpha) \in \mathcal{O}(m)$. De fato, seja $p(x) = x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ tal que $p(\alpha) = 0$, logo, $\alpha^2 + a_1\alpha = -a_0$. Então,

$$\begin{aligned} p(\sigma(\alpha)) &= [\sigma(\alpha)]^2 + a_1\sigma(\alpha) + a_0 \\ &= \sigma(\alpha^2) + \sigma(a_1\alpha) + a_0 \\ &= \sigma(\alpha^2 + a_1\alpha) + a_0 \\ &= \sigma(-a_0) + a_0 \\ &= -a_0 + a_0 = 0. \end{aligned}$$

Proposição 2.2. *Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$. O elemento α é um inteiro quadrático se e somente se $\mathcal{T}_r(\alpha)$ e $\mathcal{N}(\alpha)$ são números inteiros.*

Demonstração: Seja $\alpha \in \mathbb{Q}[\sqrt{m}]$ tal que $\mathcal{T}_r(\alpha)$ e $\mathcal{N}(\alpha)$ são números inteiros. Pela Proposição 2.1, α é raiz do polinômio $f_\alpha(x) = x^2 - \mathcal{T}_r(\alpha)x + \mathcal{N}(\alpha)$ com coeficientes em $\mathbb{Z}$. Portanto, α é um inteiro quadrático.

Seja $\alpha = a + b\sqrt{m} \in \mathcal{O}(m)$, com a, $b \in \mathbb{Q}$. Pela Observação 2.3, $\sigma(\alpha) \in \mathcal{O}(m)$. Como $\mathcal{O}(m)$ é anel, $\alpha + \sigma(\alpha) = 2a \in \mathcal{O}(m)$ e $\alpha\sigma(\alpha) = a^2 - mb^2 \in \mathcal{O}(m)$. Então, existem polinômios mônicos $f(x)$ e $h(x)$ em $\mathbb{Z}[x]$ tais que $f(2a) = 0$ e $h(a^2 - mb^2) = 0$. Além disso, $2a \in \mathbb{Q}$ e $a^2 - mb^2 \in \mathbb{Q}$. Pelo Teorema 2.3, os elementos $2a$, $a^2 - mb^2 \in \mathbb{Z}$. Portanto, $\mathcal{T}_r(\alpha)$ e $\mathcal{N}(\alpha)$ são inteiros. ■

Exemplo 2.1. Seja $\alpha = 1 + \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Note que α é raiz do polinômio $p(x) = x^2 - 2x - 1 \in \mathbb{Z}[x]$, com $\mathcal{T}_r(\alpha) = 2$ e $\mathcal{N}(\alpha) = -1$. Logo α é um inteiro quadrático.

Lema 2.1. *Dado $a \in \mathbb{Q}$, $a^2 \in \mathbb{Z}$ se e somente se $a \in \mathbb{Z}$.*

Demonstração: Seja $a = \dfrac{m}{n} \in \mathbb{Q}$, com $mdc(m, n) = 1$. Suponha que $a \in \mathbb{Z}$. Então $n \neq \pm 1$. Segue que $n^2 \neq \pm 1$ e $mdc(m^2, n^2) = 1$. Logo, $a^2 = \dfrac{m^2}{n^2} \notin \mathbb{Z}$. Contradição.
A volta é óbvia. ■

Observação 2.4. $\mathbb{Z} = \mathcal{O}(m) \cap \mathbb{Q}$.
É claro que $\mathbb{Z} \subseteq \mathcal{O}(m)$, logo, $\mathbb{Z} \subseteq \mathcal{O}(m) \cap \mathbb{Q}$.
Agora, seja $\alpha \in \mathcal{O}(m) \cap \mathbb{Q}$. Então $\alpha \in \mathbb{Q}$ e $\mathcal{N}(\alpha) = \alpha^2 \in \mathbb{Z}$. Pelo Lema 2.1 $\alpha \in \mathbb{Z}$.

Proposição 2.3. $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m};\ a, b \in \mathbb{Z}\} \subseteq \mathcal{O}(m)$

Demonstração: Seja $\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, então $\mathcal{T}_r(\alpha) = 2a \in \mathbb{Z}$ e $\mathcal{N}(\alpha) = a^2 - b^2 m \in \mathbb{Z}$, pois $a, b, m \in \mathbb{Z}$, logo $\mathbb{Z}[\sqrt{m}] \subseteq \mathcal{O}(m)$. ■

A Proposição 2.4 sugere a possibilidade de que $\mathcal{O}(m) = \mathbb{Z}[\sqrt{m}]$. Mas isso é falso como pode ser visto através do exemplo abaixo.

Exemplo 2.2.

(a) Sejam $m = 13$ e $\beta = \dfrac{1 + \sqrt{13}}{2}$. Temos que $\mathcal{T}_r(\beta) = 1$ e $\mathcal{N}(\beta) = \dfrac{1}{4} - \dfrac{1}{4} \cdot 13 = -6$. Assim $\beta \in \mathcal{O}(13)$ e $\beta \notin \mathbb{Z}[\sqrt{13}]$. Logo $\mathcal{O}(m) \nsubseteq \mathbb{Z}[\sqrt{m}]$ para $m = 13$.

(b) Seja $\gamma = \dfrac{3 + \sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$. Então $\mathcal{T}_r(\gamma) = 3$ e $\mathcal{N}(\gamma) = 1$, logo γ é um inteiro algébrico, mas $\gamma \neq \mathbb{Z}[\sqrt{5}]$, portanto $\mathcal{O}(5) \nsubseteq [\sqrt{5}]$.

Perguntas: Já que $\mathcal{O}(m) \neq \mathbb{Z}[\sqrt{m}]$, é possível caracterizar $\mathcal{O}(m)$? Existe alguma relação em comum nos dois exemplos acima?

Respostas: Sim, é possível caracterizar $\mathcal{O}(m)$. Para isso teremos de distinguir os valores de m módulo 4, e como m é livre de quadrados só poderemos ter três casos: $m \equiv 1, 2, 3 \pmod 4$. Assim a afirmação $m \not\equiv 1 \pmod 4$ significa que $m \equiv 2, 3 \pmod 4$. O fato comum entre os dois exemplos acima é que $m \equiv 1 \pmod 4$ nos dois casos ($m = 13$, $m = 5$).

Lema 2.2. *Seja $\mathcal{O}(m)$ o anel de inteiros do corpo quadrático $K = \mathbb{Q}[\sqrt{m}]$, com m livre de quadrados, sobre $\mathbb{Z}$. Se $\alpha = a + b\sqrt{m} \in \mathcal{O}(m)$, então $2a \in \mathbb{Z}$ e $2b \in \mathbb{Z}$.*

Demonstração: Se $\alpha \in \mathcal{O}(m)$, então

$$2a = \mathcal{T}_r(\alpha) \in \mathbb{Z} \text{ e } (2a)^2 - m(2b)^2 = 4(a^2 - mb^2) = 4\mathcal{N}(\alpha) \in \mathbb{Z}.$$

Logo $m(2b)^2 \in \mathbb{Z}$. Se $2b \notin \mathbb{Z}$, o seu denominador tem um fator primo p, e este fator aparece como p^2 no denominador de $m(2b)^2$. Sendo m livre de quadrados, segue que $m(2b)^2 \notin \mathbb{Z}$, o que é uma contradição. Portanto $2b \in \mathbb{Z}$. ■

Lembre que $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{ f\left(\frac{1+\sqrt{m}}{2}\right) \; ; \; f(x) \in \mathbb{Z}[x] \right\}$.

O Lema abaixo apresenta uma caracterização para os elementos de $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$.

Lema 2.3. *Seja m um inteiro livre de quadrado, $m \equiv 1 \pmod 4$. Então*

$$\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \left\{ \frac{a+b\sqrt{m}}{2} \; ; \; a, \, b \in \mathbb{Z} \;\; e \;\; \textit{têm mesma paridade} \right\}.$$

Demonstração:

Seja $t \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Então existe um polinômio $f(x) \in \mathbb{Z}[x]$ tal que $t = f(\frac{1+\sqrt{m}}{2})$. Note que quando $m \equiv 1 \pmod 4 \Rightarrow m - 1 = 4k \Rightarrow m - 1 - 4k = 0$, com $k \in \mathbb{Z}$.

Tome $g(x) = x^2 - x - k \in \mathbb{Z}[x]$.

$$\begin{aligned} g\left(\frac{1+\sqrt{m}}{2}\right) &= \frac{1+2\sqrt{m}+m}{4} - \frac{1+\sqrt{m}}{2} - k \\ &= \frac{1+m+2\sqrt{m}-2-2\sqrt{m}-4k}{4} \\ &= \frac{m-1-4k}{4} = 0. \end{aligned}$$

Temos que $g(x) \in \mathbb{Z}[x]$ é mônico. Pelo Algoritmo de Euclides $f(x) = g(x)h(x) + (ux + v)$, com $u, v \in \mathbb{Z}$. Então,

$$t = f(\frac{1+\sqrt{m}}{2}) = u(\frac{1+\sqrt{m}}{2}) + v = \frac{u+2v}{2} + \frac{u\sqrt{m}}{2} = \frac{a+b\sqrt{m}}{2};$$

$a = u + 2v$ e $b = u$, com a e b de mesma paridade.

Seja $t = \dfrac{a+b\sqrt{m}}{2}$.
Suponhamos que a e b são pares. Então $a = 2u$, $b = 2v$, com $u, v \in \mathbb{Z}$. Assim, $t = u + v\sqrt{m}$. Tome $f(x) = 2vx + (u - v)$

$$f\left(\frac{1+\sqrt{m}}{2}\right) = 2v\left(\frac{1+\sqrt{m}}{2}\right) + (u-v) = u + v\sqrt{m} = t$$

Suponhamos agora que a e b são ímpares. Então $a = 2u + 1$, $b = 2v + 1$, com $u, v \in \mathbb{Z}$. Assim $t = u + v\sqrt{m} + \dfrac{1+\sqrt{m}}{2}$. Tome $g(x) = (2v + 1)x + (u - v)$

$$g\left(\frac{1+\sqrt{m}}{2}\right) = (2v+1)\left(\frac{1+\sqrt{m}}{2}\right) + (u-v) = u + v\sqrt{m} + \frac{1+\sqrt{m}}{2} = t$$

■

Teorema 2.4. *Seja $\mathbb{Q}[\sqrt{m}]$ um corpo quadrático, com m um inteiro livre de quadrados, ou seja, $m \not\equiv 0 \pmod 4$.*

(a) Se $m \equiv 2 \pmod 4$ *ou* $m \equiv 3 \pmod 4$*, o anel* $\mathcal{O}(m)$ *dos inteiros de* $\mathbb{Q}[\sqrt{m}]$ *consiste de todos os elementos da forma* $(a + b\sqrt{m})$*, com* a*,* $b \in \mathbb{Z}$*.*

(b) Se $m \equiv 1 \pmod 4$*,* $\mathcal{O}(m)$ *consiste de todos os elementos da forma* $\frac{1}{2}(a + b\sqrt{m})$ *com* a*,* $b \in \mathbb{Z}$ *e de mesma paridade.*

Demonstração: Seja $\alpha = a + b\sqrt{m} \in \mathcal{O}(m)$. Pelo 2.2 temos que

$$a = \frac{u}{2} \text{ e } b = \frac{v}{2}, \text{ com } u, v \in \mathbb{Z}.$$

Também temos que

$$\frac{u^2 - mv^2}{4} = a^2 - mb^2 \in \mathbb{Z}, \tag{2.1}$$

logo, $u^2 - mv^2 \in 4\mathbb{Z}$.

(a) Se $m \equiv 2 \pmod 4$ ou $m \equiv 3 \pmod 4$, então u e v são pares, pois se v fosse ímpar, teríamos $v^2 \equiv 1 \pmod 4$. Como $u^2 - mv^2 \in 4\mathbb{Z}$, segue que $u^2 - m(4k+1) \in 4\mathbb{Z}$ o que implica que $u^2 - m \in 4\mathbb{Z}$, assim, $u^2 \equiv m \pmod 4$. Portanto, $m \equiv 1 \pmod 4$ ou $m \equiv 0 \pmod 4$, o que contradiz a hipótese. Sendo v par, temos que $v^2 \equiv 0 \pmod 4$ e, portanto $u^2 \in 4Z$. Assim u também é par. Logo $a, b \in \mathbb{Z}$ e $\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$ e, portanto, $\mathcal{O}(m) \subseteq \mathbb{Z}[\sqrt{m}]$. Já vimos que $\mathbb{Z}[\sqrt{m}] \subseteq \mathcal{O}(m)$. Portanto $\mathcal{O}(m) = \mathbb{Z}[\sqrt{m}]$.

(b) Se $m \equiv 1 \pmod 4$, então u e v têm a mesma paridade. De fato, da Equação (2.1) 4 divide $u^2 - mv^2$, se u for par, 4 divide u^2, então 4 divide mv^2. Mas m é livre de quadrados, então 4 divide v^2, logo, v é par. É análogo se consideramos que v é par.
Se u e v são pares, então a e $b \in \mathbb{Z}$, e portanto $\alpha = a + b\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$. Se u e v são ímpares, então $\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{m} \in \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \subseteq \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Portanto $\mathcal{O}(m) \subseteq \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Por outro lado, se

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

com a, $b \in \mathbb{Z}$. Então

$$\mathcal{T}_r(\alpha) = 2a + b \in \mathbb{Z},$$

pois a e $b \in \mathbb{Z}$. Temos que $m \equiv 1 \pmod 4$, então $4 \mid (1 - m)$.

$$\mathcal{N}(\alpha) = \frac{(2a+b)^2}{4} - \frac{mb^2}{4} =$$

$$= \frac{4a^2 + 4ab + b^2 - mb^2}{4} = \frac{4(a^2+ab) + b^2(1-m)}{4},$$

como 4 divide as duas parcelas do numerador, temos que $\mathcal{N}(\alpha) \in \mathbb{Z}$. Logo, $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] \subseteq \mathcal{O}(m)$. Portanto, $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] = \mathcal{O}(m)$ ■

Observação 2.5. Seja $\mathbb{Q}[\sqrt{m}]$ um corpo quadrático.

(a) Se $m \not\equiv 1 \pmod 4$, então $\beta = \{1, \sqrt{m}\}$ é uma base integral de $\mathbb{Q}[\sqrt{m}]$.

(b) Se $m \equiv 1 \pmod 4$, então $\beta = \left\{1, \frac{1+\sqrt{m}}{2}\right\}$ é uma base integral de $\mathbb{Q}[\sqrt{m}]$.

Exemplo 2.3.

(a) O anel de inteiros quadráticos de $\mathbb{Q}(\sqrt{5})$ é $\mathcal{O}(5) = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$. Assim $\left\{1, \frac{1+\sqrt{5}}{2}\right\}$ é uma base integral de $\mathcal{O}(5)$.

(b) O anel de inteiros quadráticos $\mathbb{Q}(\sqrt{-13})$ é $\mathcal{O}(-13) = \mathbb{Z}\sqrt{-13}$. Assim $\{1, \sqrt{-13}\}$ é uma base integral de $\mathcal{O}(-13)$.

Geralmente $\mathcal{O}(m)$ tem em relação a $\mathbb{Q}[\sqrt{m}]$ o mesmo papel que $\mathbb{Z}$ tem em relação a $\mathbb{Q}$.

Observação 2.6. $\mathbb{Q}[\sqrt{m}]$ é o corpo de frações de $\mathcal{O}(m)$. De fato, como $\mathcal{O}(m) \subseteq \mathbb{C}$ temos que o corpo de frações de $\mathcal{O}(m)$ é o menor subcorpo de $\mathbb{C}$ que contém $\mathcal{O}(m)$. Claro que $\mathbb{Q}[\sqrt{m}]$ é subcorpo de $\mathbb{C}$ que contém $\mathcal{O}(m)$. Vamos provar que é o menor.
Seja L um subcorpo de $\mathbb{C}$ tal que $\mathcal{O}(m) \subseteq L$. Segue que $\sqrt{m} \in L$. Como $\mathbb{Q}$ é o menor corpo contido em $\mathbb{C}$, temos $\mathbb{Q} \subseteq L$. Seja $u = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$, a, $b \in \mathbb{Q} \subseteq L$. Como $\sqrt{m} \in L$ vem que $a + b\sqrt{m} = u \in L$. Logo $\mathbb{Q}[\sqrt{m}] \subseteq L$.

Vimos pelo Teorema 2.3 que $\mathbb{Z}$ é integralmente fechado, o próximo teorema mostra que $\mathcal{O}(m)$ é também integralmente fechado

Teorema 2.5. *Sejam $\alpha \in \mathbb{Q}[\sqrt{m}]$ e $g(x) \in \mathcal{O}(m)[x]$ um polinômio mônico. Se $g(\alpha) = 0$, então $\alpha \in \mathcal{O}(m)$.*

Demonstração: Ver ([3] , página 5)

2.3 O anel dos inteiros de Gauss

O exemplo mais importante de um anel de inteiros quadráticos é o *anel dos inteiros de Gauss* $\mathbb{Z}[i]$. O anel $\mathbb{Z}[i]$ é o anel dos inteiros algébricos do corpo quadrático $\mathbb{Q}[i]$, sendo $i = \sqrt{-1}$. Como $-1 \equiv 3 \pmod 4$, os elementos de $\mathbb{Z}[i]$ são da forma $a + bi$, com a e $b \in \mathbb{Z}$. Vamos ver algumas propriedades particulares desse anel.

Sejam $x = a + bi, y = c + di \in \mathbb{Z}[i]$, . As operações de *adição* e de *multiplicação* de $\mathbb{Z}[i]$ estão definidas por:

$$x + y = (a + b) + (b + d)i,$$

$$xy = (ac - bd) + (ad + bc)i.$$

O elemento $\overline{x} = a - bi \in \mathbb{Z}[i]$ é o elemento conjugado de $x = a + bi \in \mathbb{Z}[i]$. Assim a norma e o traço de $\mathbb{Z}[i]$ são respectivamente:

$$\mathcal{T}_r(x) = x + \overline{x} = 2a$$

$$\mathcal{N}(x) = x\overline{x} = a^2 + b^2.$$

Proposição 2.4. *Seja $\alpha \in \mathbb{Z}[i]$. As seguintes afirmações são equivalentes:*

(i) α *é inversível em* $\mathbb{Z}[i]$;

(ii) $\mathcal{N}(\alpha) = 1$;

(iii) $\alpha \in \{-1, 1, -i, i\}$.

Demonstração:

$(i) \Rightarrow (ii)$ Sendo α inversível, existe um $\beta \in \mathbb{Z}[i]$ tal que $\alpha\beta = 1$. Conseqüentemente,

$$\mathcal{N}(\alpha) \cdot \mathcal{N}(\beta) = \mathcal{N}(\alpha \cdot \beta) = \mathcal{N}(1) = 1.$$

Como $\mathcal{N}(\alpha) \in \mathbb{N}$, segue das igualdades acima que $\mathcal{N}(\alpha) = 1$.

$(ii) \Rightarrow (iii)$: Seja $\alpha = x + yi$, tal que $1 = \mathcal{N}(\alpha) = x^2 + y^2$. As soluções desta equação em $\mathbb{Z} \times \mathbb{Z}$ são $(0, \pm 1)$ e $(\pm 1, 0)$, portanto $\alpha \in \{-1, 1, -i, i\}$.

$(iii) \Rightarrow (i)$ É claro que todo elemento de $\{-1, 1, -i, i\}$ é inversível em $\mathbb{Z}[i]$. ■

O anel dos inteiros guassianos possui propriedades algébricas muito semelhantes às do anel dos inteiros $\mathbb{Z}$, uma delas é que $\mathbb{Z}[i]$ é um anel fatorial.

Para mostrarmos que $\mathbb{Z}[i]$ é fatorial, vamos mostrar que $\mathbb{Z}[i]$ é um anel euclidiano, já que todo anel euclidiano é fatorial.

Proposição 2.5. *O anel $\mathbb{Z}[i]$ é euclidiano em relação à função norma*

$$\mathcal{N} : \mathbb{Z}[i] \to \mathbb{Z}$$

$$\alpha \mapsto \mathcal{N}(\alpha).$$

Isto é, se $\alpha, \beta \in \mathbb{Z}[i] \setminus \{0\}$ então $\mathcal{N}(\alpha\beta) \geq \mathcal{N}(\alpha)$. E se $\beta \neq 0$, então existem $\gamma, \rho \in \mathbb{Z}[i]$ tais que:

$$\alpha = \beta \cdot \gamma + \rho, \text{ com } \mathcal{N}(\rho) < \mathcal{N}(\beta).$$

Demonstração: Note que para qualquer α não nulo de $\mathbb{Z}[i]$, $\mathcal{N}(\alpha) \geq 1$. Então, se α e β são

dois inteiros de Gauss não nulos:

$$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta) \geq \mathcal{N}(\alpha).$$

Agora devemos achar um inteiro gaussiano γ tal que

$$\mathcal{N}(\alpha - \beta\gamma) < \mathcal{N}(\beta).$$

Como

$$\mathcal{N}(\beta) \cdot \mathcal{N}(\frac{\alpha}{\beta} - \gamma) = \mathcal{N}(\alpha - \beta\gamma),$$

γ deve ser tal que

$$\mathcal{N}(\frac{\alpha}{\beta} - \gamma) < 1.$$

Escreva $\dfrac{\alpha}{\beta}$ na forma

$$\frac{\alpha}{\beta} = x + yi, \;\; x, y \in Q.$$

Sejam r e s inteiros tais que

$$|x - r| \leq \frac{1}{2} \; e \; |y - s| \leq \frac{1}{2}.$$

Pondo $\gamma = r + si$ e $\rho = \alpha - \beta\gamma$, segue que $\alpha = \beta \cdot \gamma + \rho$, com

$$\mathcal{N}(\rho) = \mathcal{N}(\beta) \cdot \mathcal{N}(\frac{\alpha}{\beta} - \gamma) = \mathcal{N}(\beta) \cdot \mathcal{N}(x - r + (y - s)i)$$

$$= \mathcal{N}(\beta)[(x - r)^2 + (y - s)^2] \leq \mathcal{N}(\beta)\left(\frac{1}{4} + \frac{1}{4}\right)$$

$$= \frac{1}{2}\mathcal{N}(\beta) < \mathcal{N}(\beta)$$

■

Com esse resultado, temos também que o anel de inteiros de Gauss, é anel principal. Isto é, todo ideal de $\mathbb{Z}[i]$ é ideal principal.

Podemos fazer a seguinte pergunta: Todo anel de inteiros quadráticos é fatorial? A resposta é não. O anel $\mathbb{Z}[\sqrt{-5}]$ não é fatorial. Por exemplo, o número 21 não tem uma fatoração única de irredutíveis.

$$21 = 3 \cdot 7 = (1 + \cdot 2\sqrt{-5}) \cdot (1 - 2 \cdot \sqrt{-5}).$$

Mais adiante veremos que esses elementos são irredutíveis.

No capítulo 4 nosso objetivo é determinar alguns anéis de inteiros quadráticos que são euclidianos em relação a norma absoluta. Para uma função ϕ diferente da norma absoluta, não se sabe se existem outros anéis de inteiros quadráticos que são euclidianos. Para $\mathcal{O}(m)$ ser fatorial é suficiente, mas não é necessário, que ele seja euclidiano.

Existe alguns anéis de inteiros quadráticos que são fatoriais, mas não euclidianos.

Terminaremos este capítulo com um estudo mais detalhado do anel $\mathbb{Z}[i]$ dos inteiros de Gauss. Analizaremos como os números primos $p \in \mathbb{Z}$ se fatoram em $\mathbb{Z}[i]$.

Como $\mathbb{Z}[i]$ é euclidiano (e portanto fatorial) os conceitos de elemento primo e elemento irredutível coincidem em $\mathbb{Z}[i]$.

Lema 2.4. *Seja $\pi \in \mathbb{Z}[i]$. Se $\mathcal{N}(\pi)$ é primo em $\mathbb{Z}$, então π é primo em $\mathbb{Z}[i]$.*

Demonstração: Suponha que $\pi \neq 0$ não seja primo em $\mathbb{Z}[i]$. Segue que π é redutível em $\mathbb{Z}[i]$. Temos então que $\pi = \pi_1 \cdot \pi_2$ com π_1 e π_2 não nulos e não inversível. Logo

$$\mathcal{N}(\pi) = \mathcal{N}(\pi_1) \cdot \mathcal{N}(\pi_2)$$

com $\mathcal{N}(\pi_1) > 1$ e $\mathcal{N}(\pi_2) > 1$. Portanto $\mathcal{N}(\pi)$ não é primo em $\mathbb{Z}$. ■

Proposição 2.6. *Seja p um número primo e sejam m, $n \in \mathbb{Z}$. As seguintes condições são equivalentes:*

(i) $p = m^2 + n^2$

(ii) $m + n \cdot i$ *é um divisor próprio de p, não inversível em $\mathbb{Z}[i]$.*

Neste caso temos que $m \neq 0 \neq n$; os elementos $m + n \cdot i, m - n \cdot i$ são primos em $\mathbb{Z}[i]$ e $p = (m + n \cdot i) \cdot (m - n \cdot i)$.

Demonstração: Obviamente $\mathcal{N}(m + n \cdot i) = \mathcal{N}(m - n \cdot i) = m^2 + n^2 \geq 0$.

$(i) \Rightarrow (ii)$ De $p = m^2 + n^2$ resulta que $m \neq 0 \neq n$. Logo $m - n \cdot i$ e $m + n \cdot i$ não são invertíveis em $\mathbb{Z}[i]$, pela Proposição 2.4, e portanto são divisores próprios de p. Além disto, são primos (e portanto irredutíveis) em $\mathbb{Z}[i]$, pelo lema anterior.

$(ii) \Rightarrow (i)$ Existe $\alpha \in \mathbb{Z}[i] - \{-1, 1, -i, i\}$, isto é, α não inversivel, tal que $p = (m+n\cdot i)\cdot\alpha$, e da Proposição 2.4 resulta que $\mathcal{N}(\alpha) \neq 1 \neq \mathcal{N}(m+n\cdot i)$. Como $p^2 = \mathcal{N}(p) = \mathcal{N}(m+n\cdot i)\cdot\mathcal{N}(\alpha)$, concluimos que $\mathcal{N}(m + n \cdot i) = p$ ■

Os números primos p que satisfazem as condições equivalentes da proposição acima, para certos m, $n \in \mathbb{Z}$, são aqueles que se tornam redutíveis em $\mathbb{Z}[i]$. O seguinte teorema mostra que estes são exatamente os números primos $p \equiv 1 \pmod 4$ e $p = 2$.

Teorema 2.6. *Seja $p \in \mathbb{Z}$ um número primo positivo.*

(a) Se $p \equiv 3 \pmod 4$*, então* p *é irredutível em* $\mathbb{Z}[i]$.

(b) Se $p \equiv 1 \pmod 4$*, então existem números* m, $n \in \mathbb{Z}$, m *positivo e par,* n *ímpar, tais que* $p = (m + n \cdot i) \cdot (m - n \cdot i)$. *Os elementos* $m + n \cdot i$, $m - n \cdot i$ *são irredutíveis não associados em* $\mathbb{Z}[i]$.

(c) $2 = i \cdot (1 - i)^2$, *e* $1 - i$ *é irredutível em* $\mathbb{Z}[i]$.

Demonstração:

(a) Se p for redutível em $\mathbb{Z}[i]$ podemos escreer:

$$p = (m + ni)(r + si), \quad m, n, r, s \in \mathbb{Z} \tag{2.2}$$

com $m + ni$ e $r + si$ não inversivéis.
Segue que $1 \neq \mathcal{N}(m+ni) = m^2 + n^2$ e $1 \neq \mathcal{N}(r+si) = r^2 + s^2$. Aplicando a função norma em (2.2):

$$p^2 = (m^2 + n^2)(r^2 + s^2).$$

Logo $p = m^2 + n^2$. Obviamente, m^2 e n^2 são congruos a 0 ou 1 $\pmod 4$, logo $p = m^2 + n^2 \equiv$ 0 ou 1 e 2 $\pmod 4$; portanto $p \not\equiv 3 \pmod 4$.

(b) seja μ um gerador do grupo multiplicativo $\mathbb{Z}_p^*$ do corpo $\mathbb{Z}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$, o qual é cíclico de ordem $p - 1$. Seu único subgrupo de ordem 2 é gerado pelo elemento $-1 = \mu^{\frac{p-1}{4}}$, o qual é um quadrado em $\mathbb{Z}_p^*$, pois $4 \mid p - 1$. seja $h \in \mathbb{Z}$ um representante de $\mu^{\frac{p-1}{4}}$; então $h^2 \equiv -1 \pmod p$, ou seja, p divide $h^2 + 1 = (h + i)(h - i)$. Como $\mathbb{Z}[i]$ é fatorial, existe um elemento primo $\pi \in \mathbb{Z}[i]$ tal que $\pi \mid p$; portanto π divide $h + i$ ou $h - i$. Por outro lado, p obviamente não divide $h + i$ nem $h - i$; logo π é um divisor próprio de p. Da Proposição 2.6 resulta que existem m, $n \in \mathbb{Z} \setminus \{0\}$ tais que $p = m^2 + n^2 = (m + n \cdot i) \cdot (m - n \cdot i)$, e ambos os fatores são irredutíveis em $\mathbb{Z}[i]$. Como $p \equiv 1 \pmod 4$, m e n têm paridades diferentes. Substituindo, $m - n \cdot i$, $-n + m \cdot i$, podemos assumir que m é positivo e par e n é ímpar. Obviamente, os elementos $m + n \cdot i$e $m - n \cdot i$ não são associados em $\mathbb{Z}[i]$.

(c) Temos que $2 = (1+i)\cdot(1-i) = i(1-i)^2$ e, Pela proposição 2.6, $(1-i)$ é irredutível em $\mathbb{Z}[i]$ ■

Corolário 2.4. *Para qualquer número primo* p*, as seguintes condições são equivalentes:*

(i) Existem m, $n \in \mathbb{Z}$ *tais que* $p = m^2 + n^2$.

(ii) p *é redutível em* $\mathbb{Z}[i]$.

(iii) $p = 2$ *ou* $p \equiv 1 \pmod 4$.

3 *Unidades em anéis de inteiros quadráticos*

O objetivo desse capítulo é estudar o conjunto de todas as unidades (inversíveis) de um anel de inteiros quadráticos $\mathcal{O}(m)$.

Definição 3.1. *Os elementos de $\mathcal{O}(m)$ que são associados a 1 são chamados de unidades de $\mathcal{O}(m)$.*

Observação 3.1. Temos que $\mu \in \mathcal{O}(m)$ é associada a 1 quando existe $\mu' \in \mathcal{O}(m)$ tal que $1 = \mu\mu'$. Isto é, $\mu^{-1} = \mu' \in \mathcal{O}(m)$. Logo, o conjunto $\mathcal{O}(m)^*$ é na realidade o conjunto que chamamos de conjuntos dos elementos inversíveis de $\mathcal{O}(m)$.

Denotaremos por $\mathcal{O}(m)^*$ o conjunto de todas unidades de $\mathcal{O}(m)$. Claramente o produto de duas unidades é ainda uma unidade e $\mathcal{O}(m)^*$ é um subgrupo multiplicativo de $\mathbb{Q}[\sqrt{m}]$.

Lema 3.1. *O elemento μ pertence a $\mathcal{O}(m)^*$ se e somente se $|\mathcal{N}(\mu)|= 1$.*

Demonstração: Se $\mu \in \mathcal{O}(m)^*$ então existe um $\mu' \in \mathcal{O}(m)$ tal que $\mu\mu' = 1$, de onde vem que, $1 = \mathcal{N}(1) = \mathcal{N}(\mu\mu') = \mathcal{N}(\mu)\mathcal{N}(\mu')$ e como $\mathcal{N}(\mu)$ e $\mathcal{N}(\mu')$ são inteiros, concluímos que, $\mathcal{N}(\mu) = \pm 1$, portanto $|\mathcal{N}(\mu)| = 1$. Reciprocamente se $|\mathcal{N}(\mu)| = 1$, temos $\mathcal{N}(\mu) = \mu\overline{\mu} = \pm 1$ ou $\mu(\pm\overline{\mu}) = 1$, logo $\mu \in \mathcal{O}(m)^*$. ■

Note que, qualquer raiz da unidade, isto é, qualquer raiz do polinômio $x^n - 1$ (com $n \geq 1$) é um inteiro algébrico. Se $\zeta^n = 1$, então $\zeta^{-n} = 1$. Portanto, ζ^{-1} é raiz da unidade. Assim qualquer raiz da unidade que pertence a $\mathbb{Q}[\sqrt{m}]$ é uma unidade de $\mathcal{O}(m)$.

3.1 Unidades em anéis de inteiros quadráticos imaginários

Seja $\mathbb{Q}[\sqrt{m}]$ um corpo quadrático, onde m é um inteiro negativo livre de quadrados.

Se $m \equiv 2 \pmod 4$ ou $m \equiv 3 \pmod 4$, então o anel de inteiros quadráticos imaginário $\mathcal{O}(m)$ do corpo $\mathbb{Q}[\sqrt{m}]$ é da forma $\mathbb{Z}[\sqrt{m}]$. Para $\mu \in \mathcal{O}(m)$, $\mu = a + b\sqrt{m}$, com a, $b \in \mathbb{Z}$ temos que

$$\mathcal{N}(\mu) = a^2 - mb^2 \geq 0.$$

Para que μ seja uma unidade de $\mathcal{O}(m)$ devemos ter

$$a^2 - mb^2 = 1.$$

Se $m \leq -2$, então $b = 0$ e $a = \pm 1$. Portanto $\mu = \pm 1$.

Quando $m = -1$, temos a equação $a^2 + b^2 = 1$, implica que $a = 0$ e $b = \pm 1$ ou $b = 0$ e $a = \pm 1$. Com isso, $\mu = \pm 1$ ou $\mu = \pm i$.

Se $m \equiv 1 \pmod 4$, o anel de inteiros quadráticos imaginário de $\mathbb{Q}[\sqrt{m}]$ é $\mathcal{O}(m) = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Seja $\mu \in \mathcal{O}(m)$. Então $\mu = a + \dfrac{b}{2}(1 + \sqrt{m}) = a + \dfrac{b}{2} + \dfrac{b\sqrt{m}}{2}$, com a e b em $\mathbb{Z}$. Temos que

$$\mathcal{N}(\mu) = \left(a + \frac{b}{2}\right)^2 - m\frac{b^2}{4} \geq 0$$

Para que μ seja uma unidade de $\mathcal{O}(m)$ devemos ter

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

Se $m \leq -7$, então $b = 0$, e $2a^2 = 4$. Então $a = \pm 1$, portanto $\mu = \pm 1$.

Para $m = -3$ temos a equação $(2a + b)^2 + 3b^2 = 4$. Se $b \neq 0$ necessariamente $b = \pm 1$ e daí $(2a \pm 1) = \pm 1$. Isso leva a $a = \pm 1$ ou $a = 0$. Desses valores obtemos $\mu = \dfrac{\pm 1 \pm \sqrt{-3}}{2}$. Se $b = 0$, então $a = \pm 1$, e segue que $\mu = \pm 1$

Acabamos de provar o seguinte teorema:

Teorema 3.1. *Seja $\mathbb{Q}[\sqrt{m}]$ um corpo quadrático imaginário ($m < 0$), o grupo $\mathcal{O}(m)^*$ das unidades de $\mathcal{O}(m)$ é dado por:*

(a) Se $m = -1$ então $\mathcal{O}(m)^* = \{\pm 1, \pm i\}$

(b) Se $m = -3$ então $\mathcal{O}(m)^* = \{\pm 1, \pm\xi, \pm\xi^2\}$, onde $\xi = \dfrac{1 + \sqrt{-3}}{2}$

(c) Se $m < -3$ então $\mathcal{O}(m)^* = \{\pm 1\}$.

Observação 3.2. Se $\mathbb{Q}[\sqrt{m}]$ é um corpo quadrático imaginário, o grupo $\mathcal{O}(m)^*$ da unidades em $\mathbb{Q}[\sqrt{m}]$ é

- o conjunto das raízes quartas da unidade, quando $m = 1$,

- o conjunto das raízes sextas da unidade, quando $m = -3$,
- o conjunto das raízes quadradas da unidade, quando $m < -3$.

Em qualquer caso, $\mathcal{O}(m)^*$ é um grupo finito de ordem par cujos elementos são raízes da unidade.

3.2 Unidades em anéis de inteiros quadráticos reais

Seja $\mathbb{Q}[\sqrt{m}]$ um corpo quadrático, onde $m \geq 2$ é um inteiro livre de quadrados, e seja $\mu = a + b\sqrt{m}$, com $a, b \in \mathbb{Q}$, uma unidade de $\mathcal{O}(m)$. Os números μ, $\overline{\mu}$, $-\mu$ e $-\overline{\mu}$ são unidade de $\mathcal{O}(m)$, uma vez que $\mathcal{N}(\mu) = (a+b\sqrt{m})(a-b\sqrt{m}) = \pm 1$, e esses quatro números são $\pm a \pm b\sqrt{m}$. Para $\mu \neq \pm 1$ os quatro números μ, $\overline{\mu}$, $-\mu$ e $-\overline{\mu}$ são distintos, e um deles é maior do que os outros, e esse é maior do que 1.

Lema 3.2. *Seja $\mu = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ uma unidade de $\mathcal{O}(m)$, tal que $\mu > 1$. Então $a > 0$ e $b > 0$.*

Demonstração: Seja μ uma unidade de $\mathcal{O}(m)$, tal que

$$\mu = a + b\sqrt{m} > 1. \tag{3.1}$$

Então

$$-\mu = -a - b\sqrt{m} < -1. \tag{3.2}$$

Suponha que $\mathcal{N}(\mu) = 1$. Temos que $a^2 - b^2 m = (a+b\sqrt{m})(a-b\sqrt{m}) = 1 > 0$, então $a - b\sqrt{m} > 0$, pois $a + b\sqrt{m} > 0$. Como $a + b\sqrt{m} > 1$, segue que

$$0 < a - b\sqrt{m} < 1. \tag{3.3}$$

Multiplicando a Equação 3.3 por -1, temos que

$$-1 < -a + b\sqrt{m} < 0. \tag{3.4}$$

Das Equações 3.1 e 3.3, temos que

$$a - b\sqrt{m} < a + b\sqrt{m},$$

então, $b > 0$. E das equações 3.1 e 3.4, temos que

$$-a + b\sqrt{m} < a + b\sqrt{m},$$

logo, $a > 0$. No caso em que $\mathcal{N}(\mu) = -1$ é análogo. ■

Sendo $\mu > 1$ e real, temos que $\mu^n \to \infty$ quando $n \to \infty$. Assim o conjunto das unidades de $\mathcal{O}(m)$ é infinito.

Mostraremos que existe uma unidade μ_0 tal que o grupo das unidades de $\mathcal{O}(m)$ é precisamente $\mathcal{O}(m)^* = \{\pm\mu_0^r \ ; \ r \in \mathbb{Z}\}$. Também provaremos que o grupo das unidades de $\mathbb{Q}[\sqrt{m}]$ é isomorfo ao produto de $\mathbb{Z}$ com o grupo das raízes da unidade contidas em $\mathbb{Q}[\sqrt{m}]$. Como $\mathbb{Q}[\sqrt{m}]$ está contido em $\mathbb{R}$, as únicas raízes da unidade são ± 1. Portanto provaremos que $\mathcal{O}(m)^* \simeq \mathbb{Z}_2 \times \mathbb{Z}$.

Lema 3.3. *Seja $M \in \mathbb{R}$, $M > 1$. O intervalo $(1, M]$ contém apenas um número finito de unidades de $\mathcal{O}(m)$.*

Demonstração: Se $\mu = a + b\sqrt{m} \in (1, M]$ é uma unidade de $\mathcal{O}(m)$, pelo Lema 3.2 temos que $a > 0$ e $b > 0$. Por outro lado $a + b\sqrt{m} \leq M$ implica $2a < 2M$ e $2b < 2M$. Logo a cada unidade $\mu \in (1, M]$ corresponde um par de números inteiros $(2a, 2b) \in [1, 2M) \times [1, 2M)$. Como o número de pares de inteiros nesse conjunto é finito, também o número de unidades no intervalo será finito. ■

Lema 3.4. *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 $|x - \alpha y| < \dfrac{1}{M}$.*

Demonstração: Dado $t \in \mathbb{R}$ definimos $[t]$ como sendo o maior inteiro menor ou igual à t. Assim é claro que $0 \leq t - [t] < 1$.

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

$$\left[0, \frac{1}{M}\right) \ , \ \left[\frac{1}{M} \ , \ \frac{2}{M}\right) \ , \ \ldots, \left[\frac{(M-1)}{M} \ , \ 1\right),$$

cada um com comprimento $\frac{1}{M}$. 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 $0 < \beta_i < 1$. Temos então $M + 1$ elementos $\beta_i's$ no intervalo $[0, 1)$, e M subintervalos em $(0, 1)$, assim existem inteiros u e v, $0 < u < v \leq M + 1$, tais que β_u e β_v pertencem à um mesmo subintervalo. Isto é,

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

Chamando $x = [v\alpha] - [u\alpha]$ e $y = v - u$ temos $|x - \alpha y| < \dfrac{1}{M}$ com $x \geq 0$ e $y > 0$. ■

Lema 3.5. *Seja $\alpha > 0$ um número irracional. Existem infinitos pares de inteiros (x, y) tais que $y \neq 0$ e $\left|\dfrac{x}{y} - \alpha\right| < \dfrac{1}{y^2}$.*

Demonstração: Para $x = [\alpha]$ e $y = 1$ as condições do lema são satisfeitas. 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 $\delta = min\{|x_i - \alpha y_i| \ ; \ i = 1, \ldots, n\}$. Temos que $\delta > 0$, pois $\frac{x_i}{y_i} \in \mathbb{Q}$ e $\alpha \in \mathbb{R} - \mathbb{Q}$. Seja M um número natural tal que $\frac{1}{M} < \delta$. Pelo Lema 3.4 temos que existem $x, y \in \mathbb{Z}$ com $x \geq 0$ e $0 < y \leq M$ tais que $|x - \alpha y| < \frac{1}{M} < \delta$. Assim (x, y) é distinto de qualquer (x_i, y_i) e

$$\left|\frac{x}{y} - \alpha\right| = \frac{1}{y}|x - \alpha y| < \frac{1}{yM} \leq \frac{1}{y^2}.$$

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

O próximo teorema mostra que para todo $m \in \mathbb{N}$, $m > 1$, o anel de inteiros quadráticos $\mathcal{O}(m)$ possui unidade não trivial.

Teorema 3.2. *Para cada $m \in \mathbb{N}$, $m > 1$, existem inteiros x e y, com $y \neq 0$, tais que $x^2 - my^2 = 1$.*

Demonstração: Vamos encontrar $k \in \mathbb{Z}$ tal que $\mathcal{N}(\alpha) = k$ para um número infinito de elementos $\alpha \in \mathbb{Z}[\sqrt{m}]$.

Sejam $x, y \in \mathbb{Z}$ com $y \neq 0$ tais que

$$\left|\frac{x}{y} - \sqrt{m}\right| < \frac{1}{y^2}. \tag{3.5}$$

Temos que

$$\begin{aligned} |\mathcal{N}(x + y\sqrt{m})| &= \left|x^2 - my^2\right| = |x - y\sqrt{m}|\,|x + y\sqrt{m}| = y^2\left|\frac{x}{y} - \sqrt{m}\right|\left|\frac{x}{y} + \sqrt{m}\right| \\ &< \left|\frac{x}{y} + \sqrt{m}\right| = \left|\frac{x}{y} - \sqrt{m} + 2\sqrt{m}\right| \leq \left|\frac{x}{y} - \sqrt{m}\right| + 2\sqrt{m} \\ &< \frac{1}{y^2} + 2\sqrt{m} \leq 1 + 2\sqrt{m}. \end{aligned}$$

Portanto $\mathcal{N}(x + y\sqrt{m})$ é um inteiro entre $-1 - 2\sqrt{m}$ e $1 + 2\sqrt{m}$. Como pelo Lema 3.5, existem infinitos pares (x, y) que satisfazem (3.5), temos que existe $k \in \mathbb{Z}$, $k \neq 0$, com $|k| < 1 + 2\sqrt{m}$ e tal que $\mathcal{N}_k = \{\alpha \in \mathbb{Z}[\sqrt{m}] \ ; \ \mathcal{N}(\alpha) = k\}$. Então o conjunto $\mathcal{N}_k$ é um conjunto infinito.

Sejam $\alpha, \beta \in \mathcal{N}_k$ tais que $\alpha \neq \pm\beta$. Então $\alpha\beta^{-1} \neq \pm 1$ e $\mathcal{N}(\alpha\beta^{-1}) = \mathcal{N}(\alpha)\mathcal{N}(\beta)^{-1} = \frac{k}{k} = 1$. Assim, se encontramos α, β nessas condições e tais que $\alpha\beta^{-1} \in \mathbb{Z}[\sqrt{m}]$ o teorema está demonstrado, pois escolhemos $x + y\sqrt{m} = \alpha\beta^{-1} \in \mathbb{Z}[\sqrt{m}]$ e temos $x, y \in \mathbb{Z}$ tais que $1 = \mathcal{N}(\alpha\beta^{-1}) = x^2 - my^2$.

Observemos que $\alpha\beta^{-1} = \dfrac{\alpha\bar{\beta}}{\mathcal{N}(\beta)} = \dfrac{\alpha\bar{\beta}}{k}$. Estamos portanto procurando $\alpha, \beta \in \mathcal{N}_k$ tais que $\alpha\bar{\beta} \in k\mathbb{Z}[\sqrt{m}]$ e $\alpha \neq \pm\beta$. Seja

$$S_k = \left\{(\bar{x}, \bar{y}) \in \mathbb{Z}_{|k|} \times \mathbb{Z}_{|k|} \ ; \ \alpha = x + y\sqrt{m} \in \mathcal{N}_k\right\},$$

onde $\mathbb{Z}_{|k|}$ é o conjunto finito das classes de inteiros módulo $|k|$.
Como S_k é finito e $\mathcal{N}_k$ é infinito, existem $\alpha = x + y\sqrt{m}$ e $\beta = x' + y'\sqrt{m}$ em $\mathcal{N}_k$ tais que $\alpha \neq \pm\beta$ e (x, y) e (x', y') pertencem a mesma classe de equivalência. Isto é, k divide $x - x'$ e $y - y'$. Portanto $k \mid [x - x' + (y - y')\sqrt{m}] = \alpha - \beta$. Logo $\alpha - \beta = k\gamma$, com $\gamma \in \mathbb{Z}[\sqrt{m}]$. Assim $k\gamma\bar{\beta} = (\alpha - \beta)\bar{\beta} = \alpha\bar{\beta} - k$, (lembrando que $\mathcal{N}(\beta) = \beta\bar{\beta}$). Logo $\alpha\bar{\beta} = k(\gamma\bar{\beta} + 1) \in k\mathbb{Z}[\sqrt{m}]$ e ainda $\alpha \neq \pm\beta$. ■

3.2.1 Unidade fundamental

Teorema 3.3. *Existe uma única unidade $\mu_0 > 1$ em $\mathcal{O}(m)$ tal que toda unidade de $\mathcal{O}(m)$ é da forma $\pm\mu_0^n$ com $n \in \mathbb{Z}$.*

Demonstração: Pelo Teorema 3.2 existe pelo menos uma unidade $u \in \mathbb{Z}[\sqrt{m}]$. Sabemos que se u é uma unidade, então $-u, \pm\overline{u}$ também são unidades. Seja $w = x + y\sqrt{m}$ a unidade, entre essas, tal que $w > 1$. Mais ainda, exite apenas um número finito de unidades no intervalo $(1, w]$ pelo Lema 3.3. Tomamos então $\mu_0 = \min\{\mu \in \mathcal{O}(m)^*; \ \mu > 1\}$ e seja ν uma unidade de $\mathcal{O}(m)$ com $\nu > 1$. Como $\mu_0^k \to \infty$ com $k \in \mathbb{N}$, temos que existe n tal que $0 < \mu_0^{n-1} < \nu \leq \mu_0^n$, e pela escolha de μ_0, $n \geq 1$. Assim $0 < 1 < \nu\mu_0^{1-n} \leq \mu_0$. Novamente, pela escolha de μ_0 temos que $\nu\mu_0^{1-n} = \mu_0$, ou seja, $\nu = \mu_0^n$. Seja agora $\nu \neq \pm 1$ uma unidade qualquer de $\mathcal{O}(m)$. Temos que alguma unidade do conjunto $\{\pm\nu, \pm\overline{\nu}\} = \{\pm\nu, \pm\nu^{-1}\}$ é maior que 1. Portanto $\nu = \pm\mu_0^n$ com $n \in \mathbb{Z}$. A unicidade de μ_0 decorre da sua escolha. ■
A unidade μ_0 do teorema é chamada de *unidade fundamental* de $\mathcal{O}(m)$.

Corolário 3.1. *O grupo das unidades $\mathcal{O}(m)^*$ é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}$.*

Demonstração: Seja $\phi : \mathcal{O}(m)^* = \{\pm\mu_0^r; r \in \mathbb{Z}\} \to \mathbb{Z}_2 \times \mathbb{Z}$, definida por $\phi(\mu_0^r) = (\bar{0}, r)$ e $\phi(-\mu_0^r) = (\bar{1}, r)$. Vamos mostrar que ϕ é um isomorfismo de $\mathcal{O}(m)^*$ sobre $\mathbb{Z}_2 \times \mathbb{Z}$.
Sejam $\nu, \mu \in \mathcal{O}(m)^*$.

- Se $\nu = \mu_0^t$ e $\mu = \mu_0^s$, $t, s \in \mathbb{Z}$. Então $\phi(\nu\mu) = \phi(\mu_0^t \cdot \mu_0^s) = \phi(\mu_0^{t+s}) = (\bar{0}, t + s) = (\bar{0}, t) + (\bar{0}, s) = \phi(\mu_0^t) + \phi(\mu_0^s) = \phi(\nu) + \phi(\mu)$.

- Se $\nu = \mu_0^t$ e $\mu = -\mu_0^s$, $t, s \in \mathbb{Z}$. Então $\phi(\nu\mu) = \phi(\mu_0^t(-\mu_0^s)) = \phi(-\mu_0^{t+s}) = (\bar{1}, t + s) = (\bar{0}, t) + (\bar{1}, s) = \phi(\nu) + \phi(\mu)$.
  Para $\nu = -\mu_0^t$ e $\mu = \mu_0^s$ é análogo.

- Se $\nu = -\mu_0^t$ e $\mu = -\mu_0^s$, $t, s \in \mathbb{Z}$. Então $\phi(\nu, \mu) = \phi((-\mu_0^t)(-\mu_0^s)) = \phi(\mu_0^{t+s}) = (\bar{0}, t+s) = (\bar{1}, t) + (\bar{1}, s) = \phi(\nu) + \phi(\mu)$.

Portanto, ϕ é um homomorfismo.
Note que $Ker(\phi) = \{1\}$ e que 1 é o elemento neutro de $\mathcal{O}(m)^*$. Logo, ϕ é injetora.
Falta verificar que ϕ é sobrejetora. Seja $x \in \mathbb{Z}_2 \times \mathbb{Z}$.
Se $x = (\bar{0}, t)$, $t \in \mathbb{Z}$, tome $\nu = \mu_0^t \in \mathcal{O}(m)^*$. Então $\phi(\nu) = x$.
E se $x = (\bar{1}, s)$, $s, t \in \mathbb{Z}$, tome $\mu = (-\mu_0^s) \in \mathcal{O}(m)^*$. Então $\phi(\mu) = x$. ■

Terminaremos este capítulo com algumas informações sobre a forma de encontrar a unidade fundamental de $\mathcal{O}(m)$.

Seja $m \equiv 2 \pmod 4$ ou $m \equiv 3 \pmod 4$. Neste caso o anel dos inteiros de $\mathbb{Q}[\sqrt{m}]$ é $\mathbb{Z}[\sqrt{m}]$. Como as unidades de $\mathbb{Q}[\sqrt{m}]$ são inteiros quadráticos de norma ± 1, as unidades maiores que 1 de $\mathbb{Q}[\sqrt{m}]$ são os números $a + b\sqrt{m}$ com $a, b \in \mathbb{Z}$ e $a > 0, b > 0$ tal que

$$a^2 - mb^2 = \pm 1 \tag{3.6}$$

Observamos que as soluções (a, b) "em números naturais"da equação (3.6) (chamadas de equação de Pell-Fermat) são obtidas da seguinte forma:

Seja $a_1 + b_1\sqrt{m}$ a unidade fundamental de $\mathbb{Q}[\sqrt{m}]$, definimos

$$a_n + b_n\sqrt{m} = (a_1 + b_1\sqrt{m})^n, n \geq 1. \tag{3.7}$$

Note que a sequência $(a_n, b_n)_{n\in\mathbb{N}}$ enumera todas as soluções de (3.7).

Observação 3.3. Segue da equação (3.7) que $b_{n+1} = a_1 b_n + b_1 a_n$. Uma vez que a_1, b_1, a_n e b_n são todos inteiros positivos, a seqüência (b_n) é estritamente crescente. Então, uma forma de calcular a unidade fundamental $a_1 + b_1\sqrt{m}$, é anotar a sequência (mb^2) para $b \in \mathbb{N}$, $b \geq 1$ e parar na primeiro número mb_1^2 dessa seqüência que difere de um quadrado a_1^2 por ± 1. Assim, $a_1 + b_1\sqrt{m}$ é a unidade fundamental de $\mathbb{Q}[\sqrt{m}]$. Por exemplo, se $m = 7$, a seqüência (mb^2) é 7, 28, 63=64-1=8^2-1, então tomando $b_1 = 3$ e $a_1 = 8$, vemos que $8+3\sqrt{7}$ é a unidade fundamental de $\mathbb{Q}[\sqrt{7}]$. Podemos ver similarmente que as unidades fundamentais de $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[\sqrt{3}]$ e $\mathbb{Q}[\sqrt{6}]$ são $1 + \sqrt{2}, 2 + \sqrt{3}$, e $5 + 2\sqrt{6}$, respectivamente.

Um procedimento que pode ser mais rápido para o cálculo da unidade fundamental é utilizando a teoria de frações contínuas.

Se a unidade fundamental é de norma 1, a sequência $(a_n, b_n)_{n\in\mathbb{N}}$ é solução apenas para as equações $a^2 - mb^2 = 1$, neste caso, a equação $a^2 - mb^2 = -1$ não tem soluções em números naturais. Se a unidade fundamental tem norma -1, as soluções de $a^2 - mb^2 = 1$ compreende a sequência (a_{2n}, b_{2n}), e aquelas de $a^2 - b^2m = -1$ a sequência (a_{2n+1}, b_{2n+1}). O primeiro caso ocorre por exemplo quando $m = 3$, 6 ou 7, o segundo quando $m = 2$ ou 10 ($3+\sqrt{10}$ é a unidade fundamental em $\mathbb{Q}[\sqrt{10}]$).

Seja $m \equiv 1 \pmod 4$. Os inteiros de $\mathbb{Q}[\sqrt{m}]$ são os números $\frac{1}{2}(a + b\sqrt{m})$, com $a, b \in \mathbb{Z}$ e de mesma paridade. Conseqüentemente, se $\frac{1}{2}(a + b\sqrt{m})$ é uma unidade de $\mathbb{Q}[\sqrt{m}]$, devemos ter

$$a^2 - mb^2 = \pm 4. \tag{3.8}$$

Reciprocamente, se (a, b) é uma solução inteira de (3.8), então $\frac{1}{2}(a + b\sqrt{m})$ é um inteiro de $\mathbb{Q}[\sqrt{m}]$ (seu traço é a, e sua norma é ± 1), logo é uma unidade de $\mathbb{Q}[\sqrt{m}]$. Como no caso $m \not\equiv 1 \pmod 4$, denotamos a unidade fundamental de $\mathbb{Q}[\sqrt{m}]$ por $a_1 + b_1\sqrt{m}$, vemos que a solução em pares de números naturais (a, b) de (3.8) compreende os valores da sequência $(a_n, b_n$, com $n \geq 1)$ definida por:

$$a_n + b_n\sqrt{m} = 2^{1-n}(a_1 + b_1\sqrt{m})^n. \tag{3.9}$$

O cálculo de $a_1 + b_1\sqrt{m}$ pode ser feito da mesma forma que no caso $m \not\equiv 1 \pmod 4$. Por exemplo, a unidade fundamental de $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{13}]$, e $\mathbb{Q}[\sqrt{17}]$ são $\frac{1}{2}(1 + \sqrt{5})$, $\frac{1}{2}(3 + \sqrt{13})$, e $4 + \sqrt{17}$, respectivamente. Todas essas três unidades tem norma -1. Para a escolha do sinal $\pm$ 1 em (3.8) temos um resultado similar para aquele obtido no caso $m \not\equiv 1 \pmod 4$.

Observamos que no caso $m \equiv 1 \pmod 4$ a solução de equação de Pell-Fermat

$$a^2 - mb^2 = \pm 1$$

corresponde a unidade $a+b\sqrt{m}$ $(a, b > 0)$ que pertencem ao anel $\mathbb{Z}[\sqrt{m}]$. Este anel é um subanel do anel $\mathcal{O}(m)$ do inteiros de $\mathbb{Q}[\sqrt{m}]$ e as unidades positivas de $\mathbb{Z}[\sqrt{m}]$ forma um subgrupo G do grupo de unidades positivas de $\mathbb{Z}[\sqrt{m}]$. Seja $\mu = \frac{1}{2}(a+b\sqrt{m})$ a unidade fundamental de $\mathbb{Q}[\sqrt{m}]$. Se a e b são ambos pares, então $\mu \in \mathbb{Z}[\sqrt{m}]$, tal que G consiste das potência de μ. Se a e b são ambos ímpares, então $\mu^3 \in \mathbb{Z}[\sqrt{m}]$. Para ver isso note que $8\mu^3 = a(a^2+3b^2m)+b(3a^2+b^2m)\sqrt{m}$. Uma vez que $a^2 - b^2m = \pm 4$, $a^2 + 3b^2m = 4(b^2m \pm 1)$, o qual é multiplo de 8, uma vez que b e m são ímpares. Similarmente $3a^2 + b^2m = 4(a^2 \pm 1)$, o qual é novamente um multiplo de 8, porque a é ímpar. Neste caso G consiste das potências $\mu^3(\mu^2 \notin \mathbb{Z}[\sqrt{m}]$, ao contrário $\mu = \frac{\mu^3}{\mu^2} \in \mathbb{Z}[\sqrt{m}]$. Isso acontece, por exemplo, quando $m = 5$ (respectivamete, $m = 13$), no qual $\mu^3 = 2 + \sqrt{5}$ (respectivamente, $\mu^3 = 18 + 5\sqrt{13}$).

4 Fatoração em Irredutíveis

Sejam $\mathbb{Q}[\sqrt{m}]$ um corpo quadrático e $\mathcal{O}(m)$ o seu anel dos inteiros. Veremos nesta seção que não temos, em geral, para $\mathcal{O}(m)$ um "Teorema de Fatoração Única"em irredutíveis como temos em $\mathbb{Z}$. Iremos exibir alguns corpos quadráticos para os quais o seu anel de inteiros é euclidiano.

Exemplo 4.1. O anel $\mathcal{O}(-5) = \mathbb{Z}[\sqrt{-5}]$ não é fatorial, pois a decomposição em irredutíveis não é única. Vejamos:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Vamos provar que os fatores $1+2\sqrt{-5}$, $1-2\sqrt{-5}$, 3 e 7 são irredutíveis em $\mathcal{O}(-5)$. Como eles têm norma 21, 21, 9, 49, respectivamente, eles não são inversívies em $\mathcal{O}(-5)$. Se $1+2\sqrt{-5}$ fosse redutível, isto é, se existissem α, $\beta \in \mathcal{O}(-5) \setminus \mathcal{O}(-5)^*$ tais que $1 + 2\sqrt{-5} = \alpha\beta$, então teríamos que $21 = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, logo $\mathcal{N}(\alpha) \in \{3, -3, 7, -7\}$. Mas isto é impossível pois $\mathcal{N}(m + n\sqrt{-5}) = m^2 + 5n^2 \notin \{3, -3, 7, -7\}$, quaisquer que sejam m, $n \in \mathbb{Z}$. A irredutibilidade de $1 - 2\sqrt{-5}$, 3 e 7 é provada analogamente.

4.1 Elementos primos e irredutíveis em $\mathcal{O}(m)$

Sabemos que todo elemento primo de anel de integridade é um elemento irredutível. No anel $\mathbb{Z}$, um elemento é primo se e somente se é irredutível. E com isso é assegurado a decomposição única de fatores irredutíveis em $\mathbb{Z}$. Para os anéis $\mathcal{O}(m)$ veremos que irredutíveis e primos não coincidem em geral.

Recordamos que $\mu \in \mathcal{O}(m)^*$ é equivalente a $\mathcal{N}(\mu) = \pm 1$. E que se $\alpha \mid \beta$ e $|\mathcal{N}(\alpha)| = |\mathcal{N}(\beta)|$, então α e β são associados.

Observação 4.1.

(a) Sejam α e $\beta \in \mathcal{O}(m)$. Se $\alpha \mid \beta$, então $\mathcal{N}(\alpha) \mid \mathcal{N}(\beta)$. De fato, se $\alpha \mid \beta$, exite $\gamma \in \mathcal{O}(m)$ tal que $\beta = \alpha\gamma$, assim $\mathcal{N}(\beta) = \mathcal{N}(\alpha)\mathcal{N}(\gamma)$, logo $\mathcal{N}(\alpha) \mid \mathcal{N}(\beta)$.

(b) Se α e β são associados, então $\mathcal{N}(\alpha) = \pm\mathcal{N}(\beta)$. Seja μ um unidade tal que $\alpha = \beta\mu$, então $\mathcal{N}(\alpha) = \mathcal{N}(\beta)\mathcal{N}(\mu) = \pm\mathcal{N}(\beta)$.

Proposição 4.1. *Se $\alpha \in \mathcal{O}(m)$ e $\mathcal{N}(\alpha) \in \mathbb{Z}$ é um número primo, então α é irredutível em $\mathcal{O}(m)$.*

Demonstração: Seja $\beta \in \mathcal{O}(m)$ tal que $\beta \mid \alpha$. Então $\mathcal{N}(\beta) \mid \mathcal{N}(\alpha)$. Temos assim, $\mathcal{N}(\beta) = \pm 1$ ou $\mathcal{N}(\beta) = \pm\mathcal{N}(\alpha)$. No primeiro caso temos que $\beta \in \mathcal{O}(m)^*$ e no segundo caso, segue que β e α são associados. Assim α é irredutível. ■

Proposição 4.2. *Seja $p \in \mathbb{Z}$ um elemento primo.*

(a) Se existir $\alpha \in \mathcal{O}(m)$ tal que $\mathcal{N}(\alpha) = p$, então $p = \alpha\bar{\alpha}$ é uma fatoração de p em irredutíveis de $\mathcal{O}(m)$.

(b) Caso contrário p é irredutível em $\mathcal{O}(m)$.

Demonstração: A Proposição 4.1 assegura que o item (a) é verdadeiro. Vamos assumir que não ocorre (a) e seja $p = \gamma\beta$, com $\gamma, \beta \in \mathcal{O}(m)$. Então $p^2 = \mathcal{N}(p) = \mathcal{N}(\gamma)\mathcal{N}(\beta)$. Como $\mathcal{N}(\gamma), \mathcal{N}(\beta) \in \mathbb{Z}$ e $\mathcal{N}(\gamma) = p = \mathcal{N}(\beta)$ não ocorre, pois estamos excluindo (a), temos que $\mathcal{N}(\gamma) = \pm 1$ e $\mathcal{N}(\beta) = \pm p^2$ ou $\mathcal{N}(\gamma) = \pm p^2$ e $\mathcal{N}(\beta) = \pm 1$. Logo $\gamma \in \mathcal{O}(m)^*$ ou $\beta \in \mathcal{O}(m)^*$ e assim p é irredutível em $\mathcal{O}(m)$. ■

Corolário 4.1. *Existem infinitos irredutíveis em $\mathcal{O}(m)$.*

Demonstração: Segue do fato que existem infinitos primos p em $\mathbb{Z}$. Se não existe $\alpha \in \mathcal{O}(m)$ tal que $\mathcal{N}(\alpha) = p$, então p é irredutível em $\mathcal{O}(m)$. Caso contrário, α e $\overline{\alpha}$ são irredutíveis em $\mathcal{O}(m)$. ■

O próximo teorema mostra que toda não unidade em $\mathcal{O}(m)$ tem uma decomposição em irredutíveis em $\mathcal{O}(m)$. Em geral, essa decomposição não é única, como vimos no Exemplo 4.1, e assim os anéis $\mathcal{O}(m)$ em geral, não são fatorais.

Teorema 4.1. *Se $\alpha \in \mathcal{O}(m)$, $\alpha \neq 0$ e não unidade, então α é um produto de irredutíveis.*

Demonstração: Faremos a prova por indução sobre $|\mathcal{N}(\alpha)|$. Se $\alpha \in \mathcal{O}(m) \setminus \mathcal{O}(m)^*$ e $\alpha \neq 0$, tal que $|\mathcal{N}(\alpha)| = 2$ então α é irredutível pela Proposição 4.2. Vamos assumir que o resultado vale para todo $\alpha \in \mathcal{O}(m) \setminus \mathcal{O}(m)^*, \alpha \neq 0$, tal que $\alpha \leq |\mathcal{N}(\alpha)| < n$. Seja $\gamma \in \mathcal{O}(m) \setminus \mathcal{O}(m)^*, \gamma \neq 0$ tal que $|\mathcal{N}(\gamma)| = n$. Se γ é irredutível a afirmação vale para γ. Caso contrário, $\gamma = \alpha\beta$,

com $\alpha, \beta \notin \mathcal{O}(m)^*$. Logo $|\mathcal{N}(\gamma)| = |\mathcal{N}(\alpha)||\mathcal{N}(\beta)|$ e $|\mathcal{N}(\alpha)|, |\mathcal{N}(\beta)|$ são diferentes de 1. Assim $|\mathcal{N}(\alpha)|, |\mathcal{N}(\beta)|$ são menores do que n. Pela hipótese de indução temos que α e β são um produto de irredutíveis e portanto γ também é. ■

A seguir veremos que a fatoração em primos é única a menos de unidades para os anéis $\mathcal{O}(m)$.

Lema 4.1. *Sejam $r, s \in \mathbb{N} \setminus \{0\}$ e $\{\pi_i\}_{i=1}^r$ e $\{\rho_i\}_{j=1}^s$ famílias de elementos primos de $\mathcal{O}(m)$ tais que $\pi_1\pi_2 \cdots \pi_r = \rho_1\rho_2 \cdots \rho_s$. Então $r = s$ e para cada i, $1 \leq i \leq r$ existe um único j, $1 \leq j \leq s$ tal que π_i e ρ_j são associados em $\mathcal{O}(m)$.*

Demonstração: Vamos demonstrar por indução sobre r. Se $r = 1$, temos $\pi_1 = \rho_1\rho_2 \ldots \rho_s$ e pela definição de primo resulta que existe $1 \leq j \leq s$ tal que $\pi_1|\rho_j$. Como π_1 e ρ_j são irredutiveis também, concluímos então que π_1 e ρ_j são associados pois nenhum dos dois é uma unidade. Mas se $\pi_1 = \mu\rho_j$, com $\mu \in \mathcal{O}(m)^*$ temos que $\mu\rho_j = \rho_1\rho_2 \ldots \rho_s$. Cancelando-se ρ_j dos dois lados da igualdade obtemos uma contradição se $s > 1$, pois teremos que uma unidade de $\mathcal{O}(m)$ é produto de primos ou igual a um primo de $\mathcal{O}(m)$, no caso de $s = 2$. Assumindo agora o resultado para todo $1 \leq r \leq n$, suponhamos a igualdade $\pi_1\pi_2 \ldots \pi_r = \rho_1\rho_2 \ldots \rho_s$ com $r = n$. Novamente temos que π_1 deve dividir ρ_j para algum $1 \leq j \leq s$ e então prosseguimos como no caso $r = 1$ para cancelar π_1 e ρ_j. Obtemos então $\mu\pi_2 \ldots \pi_r = \rho_1\rho_2 \ldots \rho_{j-1}\rho_{j+1} \ldots \rho_s$, onde $\mu \in \mathcal{O}(m)^*$. Como $\mu\pi_2$ é também primo e o termo do lado esquerdo da igualdade tem $r - 1$ fatores primos, temos pela hipótese de indução que a afirmação é também verdadeira para $r = n$. ■

4.2 Anéis $\mathcal{O}(m)$ que são euclidianos

Sabemos que um domínio A é euclidiano se existir uma função $\phi : A \setminus \{0\} \to \mathbb{N}$, tal que: Para $a \neq 0$ e b em A, existem q e r em A, satisfazendo $b = aq + r$ e $r = 0$ ou $\phi(r) < \phi(a)$.

Uma função ϕ que satisfaz a condição acima é chamada função euclidiana para o domínio A.

Vamos ver a seguir uma caracterização para que $\mathcal{O}(m)$ seja euclidiano em relação a norma.

Lema 4.2. *A função $\phi(\alpha) = |\mathcal{N}(\alpha)|$ é uma norma euclidiana para $\mathcal{O}(m)$ se, e somente se, dado $\gamma \in \mathbb{Q}[\sqrt{m}]$, existe $\delta \in \mathcal{O}(m)$ tal que $|\mathcal{N}(\gamma - \delta)| < 1$.*

Demonstração: Assumindo-se que $\phi(\alpha) = |\mathcal{N}(\alpha)|$ é uma norma euclidiana, tomemos $\gamma \in \mathbb{Q}[\sqrt{m}]$, $\gamma \notin \mathcal{O}(m)$ (para $\gamma \in \mathcal{O}(m)$, então $\delta = \gamma$ verifica a afirmação). Logo, este elemento é da forma $\gamma = \dfrac{\alpha}{\beta}$, com α e β em $\mathcal{O}(m)$, $\beta \neq 0$ e $\beta \nmid \alpha$. Então existem elementos δ e ρ em $\mathcal{O}(m)$

satisfazendo $\alpha = \beta\delta + \rho$ e $|\mathcal{N}(\alpha - \beta\delta)| = |\mathcal{N}(\rho)| < |\mathcal{N}(\beta)|$. Temos que,

$$|\mathcal{N}(\beta)||\mathcal{N}(\frac{\alpha}{\beta} - \delta)| = |\mathcal{N}(\alpha - \beta\delta)| < |\mathcal{N}(\beta)|.$$

Portanto, $|\mathcal{N}(\frac{\alpha}{\beta} - \delta)| < 1$, ou equivalentemente, $|\mathcal{N}(\gamma - \delta)| < 1$.

Reciprocamente, dados $\alpha, \beta \in \mathcal{O}(m)$, $\alpha \neq 0$, seja $\gamma = \beta\alpha^{-1}$. Por hipótese, existe $\delta \in \mathcal{O}(m)$ tal que $|\mathcal{N}(\gamma - \delta)| < 1$. Multiplicando essa desigualdade por $\mathcal{N}(\alpha)$ obtemos $|\mathcal{N}(\alpha)\mathcal{N}(\gamma - \delta)| < |\mathcal{N}(\alpha)|$, e por sua vez $|\mathcal{N}(\alpha\gamma - \alpha\delta)| < |\mathcal{N}(\alpha)|$, e como $\gamma = \beta\alpha^{-1}$ temos $|\mathcal{N}(\alpha\beta\alpha^{-1} - \alpha\delta)| < |\mathcal{N}(\alpha)|$ e portanto $|\mathcal{N}(\beta - \alpha\delta)| < |\mathcal{N}(\alpha)|$.

Se $r = \beta - \alpha\delta$, temos que r e δ satisfazem as condições que fazem de $\mathcal{O}(m)$ um domínio euclidiano. ■

Nos caso em que o anel é euclidiano em relação a norma absoluta, vamos dizer que o anel é *$\mathcal{N}$-euclidiano.*

4.2.1 Os anéis euclidianos $\mathcal{O}(m)$ para $m < 0$

Utilizando o Lema 4.2 exibiremos, a seguir, uma lista de valores negativos de m para os quais $\mathcal{O}(m)$ é $\mathcal{N}$-euclidiano.

Teorema 4.2. *A função $|\mathcal{N}|$ é uma norma euclidiana para $\mathcal{O}(m)$ nos casos $m = -1, -2, -3, -7, -11$.*

Demonstração: Dividiremos em dois casos conforme tivermos $m \not\equiv 1 \pmod 4$ ou $m \equiv 1 \pmod 4$. Em ambos os casos usamos o Lema 4.2. Portanto, tomamos $\gamma \in \mathbb{Q}[\sqrt{m}]$, $\gamma \neq 0$.

Caso 1: $m \not\equiv 1 \pmod 4$, isto é, $m = -1, -2$.
Seja $\gamma = u + v\sqrt{m}$, com u, v números racionais. Existem então, números inteiros s e t tais que

$$|u - s| \leq \frac{1}{2} \quad e \quad |v - t| \leq \frac{1}{2}.$$

Para $\delta = s + t\sqrt{m} \in \mathcal{O}(m)$ tem-se que $\gamma - \delta = (u - s) + (v - t)\sqrt{m}$. Logo

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

se $m = -2, -1$.

Caso 2: $m \equiv 1 \pmod 4$, isto é, $m = -3, -7, -11$
Representamos o elemento γ sob a forma $\gamma = u + v\frac{1}{2}(1 + \sqrt{m})$, com $u, v \in \mathbb{Q}$. Note que isso sempre é possível, pois dado $\gamma = a + b\sqrt{m}$, escreva $a + b\sqrt{m} = (a - b) + 2b \cdot \frac{1}{2}(1 + \sqrt{m})$ e tome

$u = a - b$, $v = 2b$. Dado o números racional v existe um número inteiro t tal que $|v - t| \leq \frac{1}{2}$. E considerando agora o número racional $u + \frac{v}{2} - \frac{t}{2}$. Existe um número inteiro s tal que

$$\left| u + \frac{v}{2} - \frac{t}{2} - s \right| \leq \frac{1}{2}.$$

Para $\delta = s + t\frac{1}{2}(1 + \sqrt{m}) \in \mathcal{O}(m)$ tem-se que $\gamma - \delta = u + \frac{v}{2} - s - \frac{t}{2} + (\frac{v}{2} - \frac{t}{2})\sqrt{m}$. Logo

$$\begin{aligned} |\mathcal{N}(\gamma - \delta)| &= \left| \left(u + \frac{v}{2} - \frac{t}{2} - s \right)^2 - m\frac{1}{4}(v - t)^2 \right| \\ &\leq \left(u + \frac{v}{2} - \frac{t}{2} - s \right)^2 + |m|\frac{1}{4}(v - t)^2 \\ &\leq \left(\frac{1}{2} \right)^2 + |m|\frac{1}{4}\left(\frac{1}{2} \right)^2 = \frac{1}{4} + |m|\frac{1}{16} < 1, \end{aligned}$$

para $|m| < 12$. ■

Com esse resultado temos que os anéis $\mathcal{O}(m)$ para m =-1, -2, -3, -7 e -11 são fatoriais.

O próximo teorema mostra que vale a reciproca do Teorema 4.2, quando $m < 0$.

Teorema 4.3. *Se $m < 0$ e $\mathcal{O}(m)$ é $\mathcal{N}$-euclidiano, então $m = -1, -2, -3, -7$ e -11.*

Demonstração: Se $\mathcal{O}(m)$ é $\mathcal{N}$-euclidiano, pelo Lema 4.2, para cada $0 \neq \alpha = a + b\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$, existe $\beta \in \mathcal{O}(m)$,

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

tal que $|\mathcal{N}(\alpha - \beta)| < 1$.

(I) Temos que

$$|\mathcal{N}(\alpha - \beta)| = \left| (a - r)^2 - m\,(b - s)^2 \right| < 1.$$

Fazendo-se $a = \frac{1}{2}$ e $b = \frac{1}{2}$, e observando que $-m = |m|$, obtemos

$$\left| (a - r)^2 - m\,(b - s)^2 \right| = \left| \left(\frac{1 + |m|}{4} \right) + \left[\left(r^2 - r \right) + |m| \left(s^2 - s \right) \right] \right| < 1.$$

Como para todo inteiro $x \neq 0$, $x^2 - x \geq 0$, temos que $\left[(r^2 - r) + |m| \left(s^2 - s \right) \right] \geq 0$. Combinando a última desigualdade com a anterior obtemos $\dfrac{(1 + |m|)}{4} < 1$, ou então $|m| < 3$, isto é m = -1 ou -2.

(II)

$$|\mathcal{N}(\alpha - \beta)| = \left| \left(a - \frac{r}{2} \right)^2 - m \left(b - \frac{s}{2} \right)^2 \right| < 1.$$

Tomamos $a = \frac{1}{4}$ e $b = \frac{1}{4}$, obtemos

$$\left|\left(\frac{(1+|m|)}{16}\right) + \left[\left(\frac{r^2}{4} - \frac{r}{4}\right) + |m|\left(\frac{s^2}{4} - \frac{s}{4}\right)\right]\right| < 1.$$

Novamente $\frac{1}{4}\left[(r^2 - r) + |m|\left(s^2 - s\right)\right] \geq 0$ nos leva a $\left(\frac{(1+|m|)}{16}\right) < 1$. Dessa forma $|m| < 17$ e como $m \equiv 1 \pmod 4$, obtemos m = -3, -7 e -11. ■

Vimos no Exemplo 4.1 que $\mathcal{O}(-5)$ não é fatorial. Portanto $\mathcal{O}(-5)$ não é euclidiano para nenhuma função ϕ. De forma análoga ao Exemplo 4.1 pode-se provar que:

- $6 = 2 \cdot 3 = (\sqrt{-6}) \cdot (-\sqrt{-6})$ são decomposições distintas em irredutíveis de $\mathcal{O}(-6)$.
- $14 = 2 \cdot 7 = (2+\sqrt{-10})(2-\sqrt{-10})$ são decomposições distintas em irredutíveis de $\mathcal{O}(-10)$.

Segue que $\mathcal{O}(-6)$ e $\mathcal{O}(-10)$ não são fatoriais, e portanto não são euclidianos para nenhuma função ϕ.

O próximo teorema completa o estudo dos anéis $\mathcal{O}(m)$, $m < 0$, que são euclidianos.

Teorema 4.4. *Se $m < -11$ então $\mathcal{O}(m)$ não é euclidiano para nenhuma função ϕ.*

Demonstração: Primeiro observamos que se $m < -11$ então os elementos 2 e 3 são irredutíveis em $\mathcal{O}(m)$. De fato, como 2 e 3 são primos em $\mathbb{Z}$, e não existe nenhum $\pi \in \mathcal{O}(m)$, com $m < -11$, tal que $\mathcal{N}(\pi) = 2$ ou $\mathcal{N}(\pi) = 3$, segue pela Proposição 4.2 que 2 e 3 são irredutíveis em $\mathcal{O}(m)$. É imediato que 2 e 3 não são divisores em $\mathcal{O}(m)$, de $\sqrt{m}$, e nem de $\frac{1}{2}(1+\sqrt{m})$ quando $m \equiv 1 \pmod 4$.

Suponhamos que exista uma aplicação $\phi : \mathcal{O}(m) \setminus \{0\} \to \mathbb{N}$ que satisfaça as condições de um anel euclidiano e seja

$$\phi(p) = min\{\phi(\mathcal{B}(m))\},$$

onde

$$\mathcal{B}(m) = \mathcal{O}(m) \setminus (\mathcal{O}(m)^* \cup \{0\}) = \mathcal{O}(m) \setminus \{-1, 1, 0\};$$

É facil mostrar que p é irredutível em $\mathcal{O}(m)$.
Se $p \mid 2$, temos, $p = \pm 2$; se $p \nmid 2$, então existem q e $r \neq 0$ em $\mathcal{O}(m)$ tais que $2 = qp + r$, onde $\phi(r) < \phi(p)$. Logo, $r \in \mathcal{O}(m)^*$ e como $r \neq 1$ teremos $r = -1$ e então $p = \pm 3$. Em resumo, p só pode assumir quatro valores: ± 2 e ± 3. Distinguiremos agora dois casos conforme tivermos $m \not\equiv 1 \pmod 4$ ou $m \equiv 1 \pmod 4$.

(1) Como $p \nmid \sqrt{m}$ resulta que existem q_1 e $r_1 \neq 0$ em $\mathcal{O}(m)$ tais que $\sqrt{m} = q_1 p + r_1$, onde

$\phi(r_1) > \phi(p)$, logo, $r_1 = \pm 1$; ora, $q_1 = a_1 + b_1\sqrt{m}$, com a_1 e b_1 inteiros, de onde vem $b_1 p = 1$, o que é absurdo.

(2) como $p \nmid \frac{1}{2}(1+\sqrt{m})$ resulta que existem q_2 e $r_2 \neq 0$ em $\mathcal{O}(m)$ tais que $\frac{1}{2}(1+\sqrt{m} = q_2 + r_2)$, onde $\phi(r_2) < \phi(p)$, logo $r_2 = \pm 1$ e então $\frac{1}{2}(1+\sqrt{m}) = q_2 p \pm 1$; ora, $q_2 = a_2 + b_2\frac{1}{2}(1+\sqrt{m})$, com a_2 e b_2 inteiros, de onde vem $b_2 p = 1$, o que é absurdo. ■

4.2.2 Os anéis euclidianos $\mathcal{O}(m)$ para $m > 0$

O problema de determinar os anéis quadráticos reais $\mathcal{O}(m)$ que são $\mathcal{N}$-euclidiano é bastante complexo e só demonstraremos o seguinte teorema.

Teorema 4.5. *A função $|\mathcal{N}|$ é uma norma euclidiana para $\mathcal{O}(m)$ nos casos $m = 2$, 3, 5 e 13.*

Demonstração:

Caso 1: $m \not\equiv 1 \pmod 4$

Seja $\gamma = u + v\sqrt{m} \in \mathbb{Q}[\sqrt{m}]$ e considere os números interios x e y tais que

$$|u - x| \leq \frac{1}{2} \text{ e } |v - y| \leq \frac{1}{2}.$$

Seja $\delta = x + y\sqrt{m} \in \mathcal{O}(m)$, logo,

$$|\mathcal{N}(\gamma - \delta)| = |(u-x)^2 - m(v-y)^2|.$$

Temos que

$$(u-x)^2 - m(v-y)^2 \leq (u-x)^2 \leq \frac{1}{4} \quad e$$
$$-(u-x)^2 + m(v-y)^2 \leq m(v-y)^2 \leq \frac{m}{4}.$$

Portanto, se $m = 2$ ou $m = 3$, teremos $|\mathcal{N}(\gamma - \delta)| < 1$. Segue do Lema 4.2 que $|\mathcal{N}|$ é função euclidiana pra $m = 2, 3$.

Caso 2: $m \equiv 1 \pmod 4$.

Seja $\gamma = u + v\frac{1}{2}(1+\sqrt{m})$, com u e $v \in \mathbb{Q}$, um elemento qualquer de $\mathbb{Q}[\sqrt{m}]$, consideremos um númro inteiro y tal que $|v - y| \leq \frac{1}{2}$ e para este inteiro y seja $x \in \mathbb{Z}$ tal que

$$|u + \frac{v}{2} - \frac{y}{2} - x| \leq \frac{1}{2}.$$

Agora seja $\delta = x + \frac{1}{2}(1 + \sqrt{m})$ temos

$$|\mathcal{N}(\gamma - \delta)| = \left| \left(u + \frac{v}{2} - x - \frac{y}{2} \right)^2 - \frac{m}{4}(v - y)^2 \right|.$$

$$\left(u + \frac{v}{2} - x - \frac{y}{2} \right)^2 - \frac{m}{4}(v - y)^2 \leq \left(u + \frac{v}{2} - x - \frac{y}{2} \right)^2 \leq \frac{1}{4}$$

$$- \left(u + \frac{v}{2} - x - \frac{y}{2} \right)^2 + \frac{m}{4}(v - y)^2 \leq \frac{m}{4}(v - y)^2 \leq \frac{m}{16}.$$

Portanto, se $m = 5$ e $m = 13$, teremos $|\mathcal{N}(\gamma - \delta)| < 1$. Segue do Lema 4.2 que $|\mathcal{N}|$ é função euclidiana para $m = 5, 13$. ■

Com este teorema, temos que os anéis $\mathcal{O}(m)$ para $m = 2$, 3, 5 e 13 são euclidianos, e portanto fatoriais. Conforme ([3], página 12), existem somente dezesseis valores de $m > 0$ para os quais $\mathcal{O}(m)$ é euclidiano com $|\mathcal{N}|$. A saber,

2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 e 73.

Ainda não é conhecido se existe valor de $m > 0$ para o qual $\mathcal{O}(m)$ é euclidiano para alguma norma euclidiana ϕ diferente de $|\mathcal{N}|$.

5 *Ideais num anel de inteiros quadráticos*

Objetivo dessa seção é mostrar que o anel $\mathcal{O}(m)$ é fatorial se e somente se é principal. Para qualquer anel de integridade A , se A é principal então A é fatorial. Com isso o nosso trabalho será mostrar que se $\mathcal{O}(m)$ é fatorial, então $\mathcal{O}(m)$ é principal.

Lembramos que um ideal I, de um anel de integridade A, é principal se e somente se existe $b \in A$ tal que $I = Ab$. Dizemos que b gera I, e denotamos $I =< b >$. Um outro fato importante a ser lembrado, é que qualquer conjunto de ideais de algum anel, é ordenado por inclusão (parcialmente ordenado).

Primeiramente vamos ver alguns resultados gerais de ideais de um anel de integridade A.

Definição 5.1. *O produto de dois ideais I e J, de um anel de integridade A, é o ideal*

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i \,;\;\; n \in \mathbb{N},\;\; a_i \in I \;\; e \;\; b_i \in J \right\}.$$

É fácil ver que IJ é de fato um ideal de A, contido em $I \cap J$. Note que IJ é o conjunto de todas as somas finitas de produtos de um elemento de I por um elemento de J.

Definição 5.2. *Seja A um anel comutativo.*

(1) Dizemos que um ideal P de A, $P \neq A$, é um ideal primo se, sempre que $xy \in P$ implicar $x \in P$ ou $y \in P$.

(2) Um ideal M de A, $M \neq A$, é um ideal maximal se, A e M são os únicos ideais de A que contém M.

Lema 5.1. *Seja P um ideal primo não nulo de um anel comutativo A. Se I e J são ideais de A e se $IJ \subseteq P$, então $I \subseteq P$ ou $J \subseteq P$.*

Demonstração: Suponhamos que $I \nsubseteq P$ e seja a um elemento de I tal que $a \notin P$. Temos que

para todo $x \in J$, $ax \in IJ \subseteq P$ e como P é ideal primo resulta que $x \in P$. Portanto, $J \subseteq P$. ■

Proposição 5.1. *Seja p um elemento primo de um anel comutativo A. Então $< p >$ é um ideal primo próprio de A.*

Demonstração: Como p é primo, é óbvio que $< p >$ é um ideal próprio. Se $xy \in < p >$, então existe um elemento $t \in A$ tal que $xy = pt$. Segue que $p \mid xy$. Como p é primo, $p \mid x$ ou $p \mid y$. Se $p \mid x$, então $x = ps$ para algum $s \in A$, logo, $x \in < p >$. O outro caso é análogo. ■

Proposição 5.2. *Num anel de integridade A todo ideal maximal é primo.*

Demonstração: Seja M um ideal maximal de A. Sejam $a, b \in A$, com $ab \in M$. Suponhamos que $a \notin M$. Temos que $< a > +M$ é ideal de A. Como $a \notin M$, vem que $M \subsetneq < a > +M$. Logo $< a > +M = A$, pois M é um ideal maximal. Desta forma, temos que $1 = ax + my$, com $x, y \in A$ e $m \in M$. Segue que $b = abx + bm \in M$. ■

Observação 5.1. Segue da definição de ideal principal e da definição de produto de dois ideais, que se I, J e $< a >$ são ideais de um anel de integridade A tais que $< a > I = < a > J$ e se $a \neq 0$, então $I = J$. De fato, se $x \in I$ então $ax \in < a > I = < a > J$. Assim, $ax = (at_1)y_1 + \cdots + (at_n)y_n$, com $t_i \in A$, $y_i \in J$, $\forall\, i \in \{1, \cdots, n\}$. Segue que, $ax = a(t_1y_1 + \cdots + t_ny_n)$, logo, $x = t_1y_1 + \cdots + t_ny_n \in J$, pois J é ideal de A. Analogamente prova-se que $J \subseteq I$.

5.1 Ideais de $\mathcal{O}(m)$

Sejam $m \neq 1$ um número inteiro livre de quadrados e $\mathbb{Q}[\sqrt{m}]$ o corpo quadrático associado a m. Lembramos que:

$$\mathcal{O}(m) = \begin{cases} a + b\sqrt{m} & \text{se} \quad m \equiv 1 \pmod 4 \\ a + b\left(\dfrac{1+\sqrt{m}}{2}\right) & \text{se} \quad m \not\equiv 1 \pmod 4 \end{cases}$$

com $a, b \in \mathbb{Z}$. Vamos adotar a seguinte notação:

$$\xi = \sqrt{m} \text{ se } m \not\equiv 1 \pmod 4 \quad \text{e} \quad \xi = \frac{1+\sqrt{m}}{2} \text{ se } m \equiv 1 \pmod 4$$

Com essa convenção temos que $\mathcal{O}(m) = \{a + b\xi;\ a, b \in \mathbb{Z}\} = \mathbb{Z} \oplus \mathbb{Z}\xi$ para todo m inteiro livre de quadrados. Usamos o símbolo $\mathbb{Z} \oplus \mathbb{Z}\xi$ no lugar de $\mathbb{Z} + \mathbb{Z}\xi$, apenas para indicar que $\mathbb{Z} \cap \mathbb{Z}\xi = \{0\}$.

Lema 5.2. *Seja I um ideal não nulo de $\mathcal{O}(m)$, então $I \cap \mathbb{Z}$ é um ideal não nulo de $\mathbb{Z}$.*

Demonstração: Seja $\alpha \in I$, $\alpha \neq 0$. Então o número inteiro $\mathcal{N}(\alpha) = \alpha\overline{\alpha} \neq 0$ pertence a I. Logo $I \cap \mathbb{Z} \neq \{0\}$.

É óbvio que $0 \in I \cap \mathbb{Z}$. Se α, $\beta \in I \cap \mathbb{Z}$, segue que α, β pertencem a I e também a $\mathbb{Z}$. Como I é ideal, $\alpha + \beta \in I$, e é imediato que $\alpha + \beta \in I \cap \mathbb{Z}$. Agora, seja $r \in \mathbb{Z} \subseteq \mathcal{O}(m)$, então $r\alpha \in I$, logo, $r\alpha \in I \cap \mathbb{Z}$. ■

Observação 5.2. Note que existe $a \in \mathbb{Z}$, $a > 0$, tal que $I \cap \mathbb{Z} = \mathbb{Z}a$, uma vez que todo ideal de $\mathbb{Z}$ é ideal principal. Em virtude disso, a é divisor de todo número inteiro pertencente a I.

Teorema 5.1. *Para todo ideal não nulo I, do anel de inteiros quadrático $\mathcal{O}(m)$, existe um única terna ordenada $(a, b, c) \in \mathbb{N}^3$ tal que*

$$I = \mathbb{Z}a \oplus \mathbb{Z}\theta$$

onde $\theta = b + c\xi$, $a > b \geq 0$ e $a \geq c > 0$.

Demonstração: Em virtude do Lema 5.2 temos que, $I \cap \mathbb{Z}$ é um ideal de $\mathbb{Z}$ e portanto existe um inteiro positivo a tal que $I \cap \mathbb{Z} = \mathbb{Z}a$. Segue que todo elemento inteiro em I é multiplo de a. Observemos que existem em I elementos da forma $n + \hat{n}\xi$, com n, $\hat{n}$ inteiros e $\hat{n} > 0$ (por exemplo $a\xi$). Pelo Princípio da Boa Ordenação, existe um menor número natural c não nulo, tal que $n + c\xi \in I$. Seja $b \geq 0 \in \mathbb{Z}$ o resto da divisão de n por a. Segue que $\theta = b + c\xi \in I$. De fato, existem b, d inteiros positivos tal que $n = ad + b$, com $0 \leq b < a$, então $b + c\xi = n - ad + c\xi$, uma vez que $ad \in \mathbb{Z}a \subseteq I$ e $n + c\xi \in I$. Portanto

$$\theta = b + c\xi \in I,$$

onde $a > b \geq 0$ e $c > 0$.

Temos que a, c são inteiros positivos. Então pelo algoritmo da divisão, existem q e r interios positivos, tal que $a = qc + r$, onde $0 \leq r < c$. O elemento

$$a\xi - q\theta = a\xi - qb - qc\xi = -qb + r\xi$$

pertence a I. Logo, pela minimalidade de c, segue que $r = 0$. Então $c \mid a$ e $0 < c \leq a$. Temos que $\mathbb{Z}a \oplus \mathbb{Z}\theta \subseteq I$

Seja $\alpha = x + y\xi \in I$, com x e $y \in \mathbb{Z}$. Aplicando o algoritmo da divisão em y e c, temos $y = q'c + r'$, onde $0 \leq r' < c$. Logo, o elemento

$$(x + y\xi) - q'\theta = x + y\xi - q'b - q'c\xi = (x - q'b) + r'\xi$$

pertence a I. Novamente pela minimalidade de c, temos $r' = 0$. Logo, $x - q'b \in I \cap \mathbb{Z} = \mathbb{Z}a$ e então existe $q'' \in \mathbb{Z}$ tal que $x - q'b = q''a$. Assim,

$$x + y\xi = q''a + q'\theta \in \mathbb{Z}a \oplus \mathbb{Z}\theta.$$

Portanto $I \subseteq \mathbb{Z}a \oplus \mathbb{Z}\theta$.

Falta mostrar a unicidade da terna (a, b, c). Suponhamos que existe $(a', b', c') \in \mathbb{N}^3$ tal que $a' > b' \geq 0$, $a' \geq c' > 0$ e $I = \mathbb{Z}a' \oplus \mathbb{Z}\theta$', onde $\theta' = b' + c'\xi$. Segue que, $\mathbb{Z}a = I \cap \mathbb{Z} = \mathbb{Z}a'$. Logo $a = a'$. Com isso, $\mathbb{Z}\theta = \mathbb{Z}\theta$', então $\theta \in \mathbb{Z}\theta$', e existe $x \in \mathbb{Z}$ tal que $b + c\xi = \theta = x\theta' = xb' + xc'\xi$. Isso implica em $b = xb'$ e $c = xc'$, então $b' \mid b$ e $c' \mid c$. Analogamente, mostra-se que $b \mid b'$ e $c \mid c'$. Portanto $b = b'$ e $c = c'$. ■

Observação 5.3. O teorema acima nos diz que todo ideal I de $\mathcal{O}(m)$ é finitamente gerado, e o conjunto $\{a, \theta\}$ é um sistema de geradores de I em $\mathcal{O}(m)$.

Um anel A que satisfaz essa condição (todo ideal de A é finitamente gerado) é chamado de *anel noetheriano.*

Denotaremos por $\Im(I)$ o conjunto de todos os ideais de $\mathcal{O}(m)$ que contém o ideal I. Note que, se $J \in \Im(I)$, então $\Im(J) \subseteq \Im(I)$.

Corolário 5.1.

(a) Para todo número inteiro $d > 0$, a família $\Im(< d >)$ é finita.

(b) Para todo ideal não nulo I de $\mathcal{O}(m)$, a família $\Im(I)$ é finita.

(c) Para todo ideal I de $\mathcal{O}(m)$, $I \neq < 1 >$, existe um ideal maximal M em $\mathcal{O}(m)$ tal que $I \subseteq M$.

Demonstração:

(a) Seja I um ideal qualquer de $\mathcal{O}(m)$, que contenha o ideal principal $< d >$, d inteiro positivo. Pelo Teorema 5.1, $I = \mathbb{Z}a \oplus \mathbb{Z}\theta$, com $\theta = b + c\xi$, onde a, b e c satisfazem as condições $a > b \geq 0$ e $a \geq c > 0$. Temos que $d \in I$, e pela Observação 5.2 $a \mid d$, logo os elementos da terna ordenada (a, b, c) estão sujeitos às seguintes restrições:

$$0 < a \leq d, \quad 0 \leq b < a \leq d \quad e \quad 0 < c \leq a \leq d. \tag{5.1}$$

Devido a unicidade do elementos a, b e c, o números de ternas ordenada que satisfazem as condições 5.1 é d^3. Logo, o conjunto $\Im(< d >)$ é finito.

(b) Vimos na demonstração do Lema 5.2 que existe um número natural não nulo a em I. Logo, $< a > \subseteq I$ e assim $\Im(I) \subseteq \Im(< a >)$. Pelo item (a), o conjunto $\Im(I)$ é finito.

(c) Temos que o conjunto $\Im(I)$ é finito. Então $\Im(I) \setminus \mathcal{O}(m)$ é finito também e não vazio. Este conjunto é ordenado por inclusão, então existe um elemento maximal M, onde M é um ideal maximal de $\mathcal{O}(m)$. ■

Lema 5.3. *Sejam x e $y \in \mathcal{O}(m)$ e $d \neq 0$ um número inteiro tal que d é um divisor de $x\overline{x}$, $y\overline{y}$ e $x\overline{y} + \overline{x}y$ em $\mathbb{Z}$. Então d é divisor de $x\overline{y}$ e de $\overline{x}y$ em $\mathcal{O}(m)$.*

Demonstração: Consideremos o elemento $d^{-1}x\overline{y}$ do corpo $\mathbb{Q}[\sqrt{m}]$. Então

$$\mathcal{T}_r(d^{-1}x\overline{y}) = d^{-1}(x\overline{y} + \overline{x}y) \quad e \quad \mathcal{N}(d^{-1}x\overline{y}) = d^{-2}(x\overline{x}y\overline{y}).$$

Como d é divisor de $x\overline{y} + \overline{x}y$ em $\mathbb{Z}$, segue que $\mathcal{T}_r(d^{-1}x\overline{y}) \in \mathbb{Z}$, e também, como d é divisor de $x\overline{x}$ e $y\overline{y}$ em $\mathbb{Z}$, temos que $\mathcal{N}(d^{-1}x\overline{y}) \in \mathbb{Z}$. Portanto $d^{-1}x\overline{y} \in \mathcal{O}(m)$, ou seja, d é um divisor de $x\overline{y}$ em $\mathcal{O}(m)$. Segue que, $\overline{d^{-1}x\overline{y}} = d^{-1}y\overline{x} \in \mathcal{O}(m)$, então d é um divisor de $y\overline{x}$ e $\mathcal{O}(m)$. ■

Lema 5.4. *Se I é um ideal de $\mathcal{O}(m)$ gerado pelos números inteiros $a_1, a_2, \cdots, a_n$, então existe $d \in \mathbb{Z}$ tal que $I =< d >$.*

Demonstração: Basta tomar $d = mdc(a_1, a_2, \cdots, a_n)$ e levar em conta que existem números inteiros $b_1, b_2, \cdots, b_n$ tais que $b_1a_1 + \cdots + b_na_n = d$. ■

Consideremos o automorfismo σ do corpo quadrático $\mathbb{Q}[\sqrt{m}]$ definido por $\sigma(\alpha) = \overline{\alpha}$ e notemos que $\sigma(\mathcal{O}(m)) = \mathcal{O}(m)$. Logo, σ induz um automorfismo sobre $\mathcal{O}(m)$. Temos também que todo automorfismo leva ideal em ideal. Assim, se I é um ideal de $\mathcal{O}(m)$, então $\sigma(I) := \overline{I}$ é um ideal de $\mathcal{O}(m)$. Vamos chamar $\overline{I}$ de *ideal conjugado* de I. Se $I =< \alpha_1, \cdots, \alpha_n >$, então $\overline{I} = \sigma(I) =< \overline{\alpha_1}, \cdots, \overline{\alpha_n} >$, em particular, se $I = \mathbb{Z}a \oplus \mathbb{Z}\theta$, então $\overline{I} = \mathbb{Z}a \oplus \mathbb{Z}\overline{\theta}$.

Teorema 5.2. *Para todo ideal J do anel $\mathcal{O}(m)$, existe um número inteiro d tal que o ideal de $\mathcal{O}(m)$ $J\overline{J} =< d >$.*

Demonstração: Se $J = \{0\}$, basta escolher $d = 0$. Suponhamos $J \neq 0$. Pelo Teorema 5.1, $J =< a, \theta >$. Logo $\overline{J} =< a, \overline{\theta} >$, e

$$J\overline{J} =< a^2, a\overline{\theta},\ a\theta,\ \theta\overline{\theta} > .$$

O ideal $I =< a^2, a\theta + a\overline{\theta}, \theta\overline{\theta} > \subseteq J\overline{J}$. Observamos que os números $a^2, a(\theta + \overline{\theta}), \theta\overline{\theta}$ são números inteiros, pois são respectivamente $\mathcal{N}(a), a\mathcal{T}_r(\theta)$ e $\mathcal{N}(\theta)$. Se $d = mdc(a^2, a(\theta + \overline{\theta}), \theta\overline{\theta})$, então

$I =< d >$ ideal de $\mathcal{O}(m)$. Como d é divisor de $a^2, a\overline{\theta} + a\theta$ e $\theta\overline{\theta}$, pelo Lema 5.3, d é divisor de $a\theta$ e $a\overline{\theta}$ em $\mathcal{O}(m)$, então d divide todos os elementos de $J\overline{J}$, ou seja $J\overline{J} \subseteq < d >$. ■

Consideremos o conjunto $\Gamma = \Gamma(\mathcal{O}(m))$ de todos os ideais não nulos do anel de inteiros quadráticos $\mathcal{O}(m)$. Temos que Γ é parcialmente ordenado por inclusão. E como $\mathcal{O}(m)$ é comutativo, temos que Γ também é comutativo.

Corolário 5.2. *Sejam J, N e M elementos de Γ. Se $JN = JM$, então $N = M$.*

Demonstração: Se $JN = JM$, com N e M em Γ, temos que $(\overline{J}J)N = (\overline{J}J)M$. Então existe d inteiro não nulo tal que $\overline{J}J =< d >$ ideal de $\mathcal{O}(m)$. Segue que $< d > N =< d > M$, pela Observação 5.1 temos $N = M$. ■

Lema 5.5. *Seja $I \neq \{0\}$ um ideal de $\mathcal{O}(m)$, seja α um elemento não nulo de $\mathcal{O}(m)$ e suponhamos que $I \subseteq < \alpha >$. Então existe um ideal J de $\mathcal{O}(m)$ tal que $I =< \alpha > J$.*

Demonstração: Seja N o conjunto de todos os elementos $\alpha^{-1}x$, com $x \in I$. Temos $N \subseteq \mathbb{Q}[\sqrt{m}]$. Então $J = \mathcal{O}(m) \cap N$ é ideal de $\mathcal{O}(m)$. De fato, o elemento nulo pertence a I, logo $0 = \alpha^{-1}0 \in N$. Portanto $0 \in J$. Sejam β , $\gamma \in J$ e $x, y \in I$ tais que $\beta = \alpha^{-1}x$ e $\gamma = \alpha^{-1}y$. Então $\beta + \gamma = \alpha^{-1}x + \alpha^{-1}y = \alpha^{-1}(x + y) \in \mathcal{O}(m)$, e $x + y \in I$, portanto, $\beta + \gamma \in J$. Para $\rho \in \mathcal{O}(m)$, temos $\rho\beta = \rho\alpha^{-1}x = \alpha^{-1}\rho x \in \mathcal{O}(m)$, com $\rho x \in I$, logo, $\rho\beta \in J$.

Observando que $x = \alpha(\alpha^{-1}x)$, concluímos que $I \subseteq < \alpha > J$. Por outro lado, evidente que $< \alpha > J \subseteq I$. ■

Teorema 5.3. *Quaisquer que sejam os elementos I e J de Γ, tem-se $I \subseteq J$ se e somente se existe $N \in \Gamma$ tal que $I = NJ$.*

Demonstração: É imediato que $NJ = I$ implica que $I \subseteq NJ \subseteq J$. Reciprocamente, pelo Teorema 5.2 e do fato que $I \subseteq J$ segue que $I\overline{J} \subseteq J\overline{J} =< d >$, para algum $d \in \mathbb{Z}$ não nulo. Pelo Lema 5.5, existe um ideal N tal que $I\overline{J} =< d > N$, de onde vem, $I(\overline{J}J) =< d > NJ$, ou seja $< d > I =< d > NJ$. Pela Observação 5.1 temos $I = NJ$. ■

Corolário 5.3. *Todo ideal primo do anel quadrático $\mathcal{O}(m)$ é um ideal maximal.*

Demonstração: Sejam P um ideal primo de $\mathcal{O}(m)$ e M um ideal de $\mathcal{O}(m)$ tais que $P \subsetneq M \subseteq \mathcal{O}(m)$. Pelo Teorema 5.3 existe um ideal R de $\mathcal{O}(m)$ tal que $MR = P$. Temos que $MR \subseteq P$ e como P é um ideal primo e $M \nsubseteq P$, segue do Lema 5.1 que $R \subseteq P$. Temos que $P \subseteq MR \subseteq R$,

então $R = P$. Portanto, $MP = P =< 1 > P$ e, neste caso, $M =< 1 >= \mathcal{O}(m)$ pelo Corolário 5.2. ■

Teorema 5.4. *(a) Todo ideal próprio I do anel quadrático $\mathcal{O}(m)$ é igual a um produto de ideais maximais de $\mathcal{O}(m)$.*

(b) Se

$$P_1P_2\cdots P_s = M_1M_2\cdots M_t \tag{5.2}$$

onde cada P_i e cada M_j são ideais maximais, então $s = t$ e, a menos da ordem dos fatores, $P_i = M_i$ para $i = 1, 2, \cdots, s$.

Demonstração:

(a) Faremos por indução finita sobre o número $f(I)$ de elementos do conjunto finito $\Im(I)$. Para $f(I) = 2$, os únicos ideais de $\Im(I)$ são o anel $\mathcal{O}(m)$ e o próprio ideal I, isto é, os únicos ideais que contêm I são ele mesmo e o anel $\mathcal{O}(m)$. Então I é um ideal maximal. Suponhamos, então que $f(I) \geq 2$ e que o item (a) seja verdadeiro para todo ideal próprio N tal que $2 \leq f(N) < f(I)$. De acordo com o Corolário 5.1, existe um ideal maximal P_1 tal que $I \subseteq P_1$ e então, pelo Teorema 5.3 existe um ideal N tal que $I = P_1N$. Notando-se que $I \subseteq N$ e $I \neq N$, temos $f(N) < f(I)$. Portanto, de acordo com a hipótese de indução, existem ideais maximais $P_2, \cdots, P_s$ tais que $N = P_2\cdots P_s$, de onde vem, $I = P_1P_2\cdots P_s$.

(b) A demonstração será por indução finita sobre o número natural não nulo s. Lembre que pela Proposição 5.1 os ideais maximais são primos. Para $s = 1$ tem-se $P_1 = M_1, \cdots M_t$. Então, pelo Lema 5.1, para algum i temos $M_i \subseteq P_1$, como M_i é um ideal maximal, então $P_1 = M_i$. Sem perda de generalidade vamos supor $i = 1$, então $M_1 = M_1M_2\cdots M_t$, portanto $t = 1 = s$. Suponhamos, então, que $s > 1$ e que a parte (b) seja verdadeira para $s - 1$. Da equação 2 resulta que $P_1P_2\cdots P_s \subseteq M_1$ logo, de acordo com o Lema 5.1, existe um índice i, com $1 \leq i \leq s$, tal que $P_i \subseteq M_i$ e então $P_i = M_i$ (pois, P_i e M_1 são ideais maximais). Sem perda de generalidade podemos supor que $i = 1$ e então

$$P_1P_2\cdots P_s = P_1M_2\cdots M_t.$$

Logo,

$$P_2\cdots P_s = M_2\cdots M_t,$$

pelo corolário 5.2. Portanto, conforme a hipótese de indução, temos $s-1 = t-1$ e $P_i = M_i$ para $i = 2, \cdots, s$ (com a notação conveniente). Em resumo, temos $s = t$ e $P_i = M_i$ para $i = 1, 2, \cdots, s$. ■

Teorema 5.5. *O anel quadrático $\mathcal{O}(m)$ é fatorial se e somente se, $\mathcal{O}(m)$ é principal.*

Demonstração: Já sabemos que todo anel principal é fatorial. Suponhamos que $\mathcal{O}(m)$ seja fatorial. Inicialmente vamos mostrar que todo ideal maximal M de $\mathcal{O}(m)$ é principal. Seja $\alpha \in M$, $\alpha \neq 0$, então existem elementos irredutíveis (primos) $\pi_1, \pi_2, \cdots, \pi_r \in \mathcal{O}(m)$ tais que $\alpha = \pi_1 \cdots \pi_r$. Como todo ideal maximal é primo, temos que M é um ideal primo. Logo, pelo menos um dos fatores π_i pertence a M. Então $< \pi_i > \subseteq M$, e pela Proposição 5.1 o ideal principal $< \pi_i >$ é primo. Segue que $< \pi_i >$ é maximal e então $M =< \pi_i >$.

Seja I um ideal próprio de $\mathcal{O}(m)$, então, pelo item (a), existem ideais maximais $P_1, P_2 \cdots P_s$ tais que $I = P_1 P_2 \cdots P_s$, e como cada P_i é principal concluímos que I também é ideal principal. ■

Um domínio que seja integralmente fechado, noetheriano e todo ideal primos não nulo é maximal, é chamado de *domínio de Dedekind*. Portanto, $\mathcal{O}(m)$ é um domínio de Dedekind, pelo Teorema 2.5, pela Observação 5.3 e pelo Corolário 5.3.

Observação 5.4. O último teorema é válido para todo domínio de Dedekind, conforme ([6], página 109).

Terminamos o trabalho com informações sobre ideais fracionários e grupos de classes, que são ferramentas para decidir se $\mathcal{O}(m)$ é fatorial. Estes resultados podem ser vistos em [7], [3] e [8].

Um conjunto $\mathfrak{a}$ de $\mathbb{Q}[\sqrt{m}]$ é chamando de *ideal fracionário* de $\mathcal{O}(m)$, se existe um $d \in \mathcal{O}(m) \setminus \{0\}$ tal que $d\mathfrak{a} \subseteq \mathcal{O}(m)$.

Se todo ideal de $\mathcal{O}(m)$ é principal, então os ideais fracionários são da forma $d^{-1} < x >= d^{-1}x\mathcal{O}(m)$ onde $d^{-1}x$ é um gerador. Isto significa que os ideais fracionários em um domínio principal $\mathcal{O}(m)$ são exatamente $\alpha\mathcal{O}(m)$, onde $\alpha \in \mathbb{Q}[\sqrt{m}]$.

Seja $\mathcal{F}$ o conjunto de todos os ideais fracionários não nulos de $\mathcal{O}(m)$. Temos que $\mathcal{F}$ é um grupo abeliano com operação a de multiplicação de ideais fracionários, tendo $\mathcal{O}(m)$ como elemento neutro. Seja $\mathcal{P}$ o subconjunto de $\mathcal{F}$ dos ideais fracionários principais. Claramente $\mathcal{P}$ é um subgrupo de $\mathcal{F}$. Podemos tomar o grupo quociente $\mathcal{C}l(m) = \mathcal{F}/\mathcal{P}$ chamado de *Grupo de Classes* de $\mathcal{O}(m)$.

Mostra-se que o grupo de classe $\mathcal{C}l(m)$ de $\mathcal{O}(m)$ é finito. Seja h a ordem de $\mathcal{C}l(m)$. Assim, para todo ideal fracionário $\mathfrak{a}$ de $\mathcal{O}(m)$ tem-se que $\mathfrak{a}^h$ um ideal principal. Portanto, quando $h = 1$, temos que todo ideal fracionário $\mathfrak{a}$ de $\mathcal{F}$ é principal, e com isso todo ideal de $\mathcal{O}(m)$ é principal. Estuda-se o grupo de classes para saber quando um anel de inteiros quadráticos $\mathcal{O}(m)$ é um anel

principal. Porém, o grande problema sobre os grupos de classes é certamente determinar h, ou mesmo se $h > 1$.

Usando essa teoria pode ser mostrar que para m =-19, -43, -67 e -163, os anéis $\mathcal{O}(m)$ são principais. É possível mostrar que os nove valores -1, -2, -3, -7, -11, -19, -43, -67 e -163 são os únicos valores de $m < 0$ para os quais $\mathcal{O}(m)$ é um domínio de ideais principais (fatoriais).

Para $0 < m < 100$, os anéis de inteiros quadráticos $\mathcal{O}(m)$ são fatoriais para os seguintes valores de m:

2, 3, 5, 6, 7, 11, 13, 14, 17, 19, 21, 22, 23, 29, 31, 33, 37, 38, 41, 43, 43, 47, 53, 57, 59, 61, 62, 67, 69, 71, 73, 77, 83, 86, 89, 93, 94 e 97.

Conclusão

No presente trabalho, definimos um corpo quadrático K como um corpo de números algébricos de grau 2. Todo corpo quadrático possui um elemento primitivo distinguido da forma $\sqrt{m}$, em que m é um inteiro livre de quadrados, isto é, vimos que $K = \mathbb{Q}[\sqrt{m}]$. Além disso caracterizamos o anel $\mathcal{O}(m)$ pelo número inteiro m módulo 4 em que $\mathcal{O}(m)$ é o anel de inteiros do corpo $\mathbb{Q}[\sqrt{m}]$.

Vimos também que o conjunto $\mathcal{O}(m)^*$ das unidades do anel $\mathcal{O}(m)$ é um grupo multiplicativo finito quando m é um inteiro negativo. E quando m é um interio positivo, o grupo $\mathcal{O}(m)^*$ é isomorfo ao produto de $\mathbb{Z}$ com o grupo das raízes da unidade contidas em $\mathbb{Q}[\sqrt{m}]$.

Observamos que todo anel euclidiano é fatorial, assim analizamos para quais valores de m o anel $\mathcal{O}(m)$ é euclidiano. Demonstramos para quais valores de $m < 0$ o anel $\mathcal{O}(m)$ é euclidiano. Por outro lado, aumenta a dificuldade para determinar os valores de m positivos para os quais o anel $\mathcal{O}(m)$ é euclidiano. Por tais razões, provamos apenas para alguns valores.

Demonstramos que todo ideal de $\mathcal{O}(m)$ é finitamente gerado por $\{a, \theta\}$, com $a \in \mathbb{Z}$ e $\theta \in \mathcal{O}(m)$. E por fim, que $\mathcal{O}(m)$ é fatorial se e somente se $\mathcal{O}(m)$ é principal.

Esse trabalho abriu portas para o estudo do grupos de classes de $\mathcal{O}(m)$, incentivou a pesquisa da Teoria dos Números Algébricos. Além de dar-me fundamentos teóricos para uma futura pós-graduação.

APÊNDICE A

Em toda esse apêndice consideramos A um anel de integridade.

A.1 Divisibilidade

Definição A.1. *Um elemento $a \in A$ é inversível quando existe um elemento $b \in A$ tal que $ab = ba = 1$, onde 1 é a unidade de A.*

Definição A.2. *Dados $a, b \in A \setminus \{0\}$, dizemos que a divide b, e denotamos por $a \mid b$, quando $c \in A$ tal que $b = ac$.*

Definição A.3. *Sejam a e b elementos de A. Dizemos que a é associado a b se $a \mid b$ e $b \mid a$. Essa relação em A será indicada por $a \sim b$.*

Proposição A.1. *Para dois quaisquer elementos a e b de A são equivalentes as seguintes afirmações:*

(i) $a \sim b$;

(ii) existe um elemento inversível $u \in A$ tal que $b = au$.

Demonstração:

$(i) \Rightarrow (ii)$ Como a é associado a b, então existem $x, y \in A$ tais que $b = ax$ e $a = by$. Temos então que $b = byx$ e isso implica que $yx = 1$, e portanto x e y são inversíveis.

$(ii) \Rightarrow (i)$ Do fato que $b = au$, com u inversível. Segue direto que $a \mid b$, segue ainda que $a = bu^{-1}$, em que u^{-1} é um elemento de A, logo $b \mid a$ ■

A.2 Máximo divisor comum

Definição A.4. *Dizemos que um elemento $d \in A$ é máximo divisor comum (mdc) dos elementos $a_1, \cdots, a_n \in A$ se:*

(1) $d \mid a_i$ *para todo* $i \in \{1, \cdots, n\}$,

(2) todo divisor de $a_1, \cdots, a_n$, *é divisor de* d *(ou seja, se* $d_1 \in A$ *e* $d_1 \mid a_i \ \forall i \in \{1, \cdots, n\}$, *então* $d_1 \mid d$*).*

Proposição A.2. *Seja* d *um mdc de* $a_1, \cdots, a_n \in A$. *Temos que* d' *é um mdc de* $a_1, \cdots, a_n$ *se e somente se* $d \sim d'$.

Demonstração: Suponha que d e d' sejam dois máximos divisores comuns de $a_1, \cdots, a_n$. Logo pelo item (i) da definição de mdc, temos que d e d' são divisores de $a_1, \cdots, a_n$ e portanto pelo item (ii) da definição de *mdc*, segue que $d \mid d'$ e $d' \mid d$, isto é, $d \sim d'$.

Reciprocamente, suponha que d seja um mdc de $a_1, \cdots, a_n$ e que $d \mid d'$ e $d' \mid d$. Como $d \mid a_i \forall i \in \{1, \cdots, n\}$ e $d' \mid d$, segue que $d' \mid a_i \ \forall i \in \{1, \cdots, n\}$. Seja agora $c \in A$ um divisor comum da $a_1, \cdots, a_n \in A$, logo pelo item (ii) da definição de *mdc*, temos que $c \mid d$ e como $d \mid d'$, segue que $c \mid d'$. Temos portanto que d' é um mdc de $a_1, \cdots, a_n \in A$. ■

Definição A.5. *Elementos de* A *se dizem primos entre si se a unidade do anel é máximo divisor comum desses elementos.*

A.3 Elementos primos e irredutíveis

Definição A.6. *Um elemento* $p \in A$ *se diz primo se:*

(1) $p \neq 0$;

(2) p *não é inversível;*

(3) quaisquer que sejam $a, b \in A$, *se* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$.

Mostra-se por indução que se p é primo e $p \mid a_1 \cdots a_n$, $n \geq 1$, então p divide um dos fatores.

Definição A.7. *Um elemento* $p \in A$ *se diz irredutível se:*

(1) $p \neq 0$;

(2) p *não é inversível;*

(3) quaisquer que sejam $a, b \in A$, *se* $p = ab$, *então* a *é inversível ou* b *é inversível.*

Por indução, prova-se que, se p é irredutível e $p = a_1 \cdots a_n$, $n \geq 1$,então p é associado a um dos fatores do segundo membro e o produto dos demais fatores é inversível.

Um elemento $p \in A$ tal que $p \neq 0$, p não é inversível e p não é irredutível é chamado *redutível*.

Proposição A.3. *Todo elemento primo de um anel de integridade A é também irredutível.*

Demonstração: Seja $p \in A$ um elemtento primo. Precisamos provar apenas a condição (iii).

Sejam $a, b \in A$ tais que $p = ab$. Logo $p \mid ab$ e então $p \mid a$ ou $p \mid b$ por definição. Se $p \mid a$, existe um elemento $c \in A$ tal que $a = pc$. A igualdade $p = ab$ se transforma em $p = pcb$, resultando $1 = cb$ e b um elemento inversível de A. Analogamente, se $p \mid b$ teríamos que a é um elemento inversível de A. ■

A.4 Anéis fatoriais

Definição A.8. *Dizemos que um anel de integridade A é um anel fatorial se e somente se, são válidas as seguintes condições:*

(1) Para todo elemento não nulo e não inversível $a \in A$ existem elementos irredutíveis $p_1, p_2, \cdots, p_s$ em A tais que

$$a = p_1 p_2 \cdots p_s;$$

(2) Sejam $\{p_i\}_{i=1}^{s}$ e $\{q_j\}_{j=1}^{t}$ famílias de irredutíveis de A. Se $a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$, então $s = t$ e existe uma permutação σ de $\{1, 2, \cdots, s\}$ tal que

$$p_1 \sim q_{\sigma(i)} \text{ para } i = 1, 2, \cdots, s.$$

A condição (2) exprime o fato que a decomposição de a, cuja existência é assegurada pela condição (1), é única a menos da ordem dos fatores irredutíveis e a menos de elementos inversíveis.

Teorema A.1. *Um anel de integridade A é um anel fatorial se e somente se, A satisfaz a condição (1) e a seguinte condição*

(2)' para todo $p \in A$, se p é irredutível, então p é primo.

Demonstração: Suponha que A seja um anel fatorial, logo, por definição, A satisfaz a condição (1).

Seja p um elemento irredutível em A e sejam a e b dois elementos de A não nulos e não inversíveis tais que $p \mid ab$; de acordo com (1) existem elementos irredutíveis $p_1, p_2 \cdots, p_s, q_1, q_2 \cdots, q_t$ tais que

$$a = p_1 p_2 \cdots, p_s \quad e \quad b = q_1 q_2 \cdots q_t$$

e como $p \mid ab$ resulta que existe $c \in A$ tal que

$$pc = p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t. \tag{A.1}$$

Em virtude da condição (2), p é associado a um dos fatores irredutíveis do segundo membro de A.1, isto é, existe um índice i ou um índice j, com $1 \leq i \leq s$ e $1 \leq j \leq t$, tal que $p \sim p_i$ ou $p \sim q_j$ de onde vem, $p \mid p_i$ ou $p \mid q_j$, logo, $p \mid a$ ou $p \mid b$.

Reciprocamente, seja A um anel de integridade que satisfaça as condições (1) e (2)', e sejam $p_1, p_2 \cdots, p_s, q_1, q_2 \cdots, q_t$ elementos irredutíveis de A e suponhamos que

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{A.2}$$

Precisamos mostrar que $s = t$ e que $p_i \sim q_{\sigma(i)}$ para $i = 1, 2, \cdots, s$. Faremos por indução finita sobre o número natural s. Para $s = 1$, temos $p_1 = q_1 q_2 \cdots q_t$ e como p_1 é irredutível resulta $t = 1$, logo $p_1 = q_1$. Suponhamos, então, que $s > 1$ e que a condição (2) seja verdadeira para $s - 1$. Da igualdade A.2 vem $p_1 \mid (q_1 q_2 \cdots q_t)$ e como p_1 é primo resulta que existe um índice i, com $1 \leq i \leq t$, tal que $p_1 \mid q_i$. Sem perda de generalidade supomos que $i = 1$, logo $p_1 \mid q_1$ e daqui concluímos que $q_1 = up_1$, onde u é um elemento inversível de A. Pondo-se $p_2' = up_2$ e cancelando o fator q_1 em A.2, temos

$$p_2' p_3 \cdots p_s = q_2 q_3 \cdots q_t,$$

onde os fatores $p_2', p_3, \cdots, p_s, q_2, q_3, \cdots, q_t$ são irredutíveis, logo, em virtude da hipótese de indução, temos $s - 1 = t - 1$ e, com uma notação conveniente, $p_2' \sim q_2', \cdots, p_s \sim q_s$, portanto, $s = t$ e $p_i \sim q_i$ para $i = 1, 2, \cdots, s$. ■

Observação A.1. Com esse resultado temos que num anel fatorial, o elemento p é irredutível se e somente se p é primo.

A.5 Anéis principais

Definição A.9. *Um anel de integridade A é dito principal quando todos os seus ideais são principais. Ou seja, se I é um ideal em um anel principal, então existe $a \in I$ tal que $I =< a >$.*

Proposição A.4. *Em um anel principal A todo elemento irredutível é primo.*

Demonstração: Seja p um elemento irredutível de A. Temos $p \neq 0$ e p não é inversível. Suponhamos que $p \mid ab$. Precisamos mostrar que $p \mid a$ ou $p \mid b$.

Seja $I =< a, p >$ o ideal de A gerado por a e p. Como A é principal, então $I =< d >$,

$d \in I$. Mas $p \in I$. Logo, existe $c \in A$ tal que $p = dc$. Como p é irredutível, então d ou c é inversível.

Se d é inversível, segue que $< d >= A$. Assim, $< a, p >= A$, o que implica que $1 = ax + py$ com x , $y \in A$. Desta forma, $b = abx + pby$, como p divide as duas parcelas da direita, segue que $p \mid b$.

Se c for inversível, segue que como $p = dc$ então $d = pc^{-1}$. Como $a \in I$, então $a = dq$, $q \in A$. Segue que $a = qpc^{-1}$ e assim $p \mid a$. Logo, p é primo. ■

Proposição A.5. *Seja A um anel principal. Então $p \in A \setminus \{0\}$ é irredutível se, e somente se, $< p >$ é maximal.*

Demonstração: Suponhamos p irredutível. Por hipótese, temos que $p \neq 0$ e p é não inversível. Vamos supor que $< p > \subset < a >$, $a \in A$. Assim, $p \in < a >$, ou seja $p = aq$, $q \in A$. Como p é irredutível segue que a ou q é inversível. Se a é inversível então $< a >= A$. Se q for inversível, temos que $a = pq^{-1}$, $q^{-1} \in A$. Então $a \in < p >$ e assim $< a > \subset < p >$. Segue que $< a >=< p >$. Logo, $< p >$ é maximal.
Reciprocamente, suponhamos que $< p >$ é maximal. Assim, $< p >\neq A$. Logo, $p \neq 0$ e p não é inversível. Suponhamos que $p = ab, a, b \in A$. Então $p \in < a >$, ou seja, $< p > \subseteq < a > \subseteq A$. Como $< p >$ é maximal segue que $< p >=< a >$, ou $< a >= A$. Se $< p >=< a >$ então p é associado a a e assim, $a = up$, $u \in A^*$. Portanto, $p = upb$ e assim $1 = ub$, ou seja, b é inversível. Se $< a >= A$, então a é inversível pois $1 = ax$, $x \in A$. Desta forma, segue que p é irredutível. ■

Lema A.1. *Seja $I_1 \subseteq I_2 \subseteq I_3 \cdots$ uma sequência de ideias em um anel principal A. Então existe um índice $t \geq 1$ tal que $I_t = I_{t+1} = \cdots$, ou seja, a sequência é estacionária.*

Demonstração: Vamos verificar primeiro que o conjunto

$$I = \bigcup_{j \geq 1} I_j$$

é um ideal de A. De fato, se x, $y \in I$, então existem índices m, n tais que $x \in I_m$ e $y \in I_n$. Fazendo $s = max\{m, n\}$, temos x, $y \in I_s$ e, por conseguinte, $x - y \in I_s$. Logo, $x - y \in I$. Se $x \in I$, então existe um r tal que $x \in I_r$. Seja $a \in A$, então $ax \in I_r$, portanto $ax \in I$.

Como A é principal, existe $d \in A$ tal que

$$I = \bigcup_{j \geq 1} I_j =< d > .$$

O fato de $d \in I$ implica que existe um índice t tal que $d \in I_t$. Portanto, $I =< d > \subseteq I_t$. Como

$I_t \subseteq I$, então $I = I_t$. Assim, $I_t = I_{t+1} = \cdots$. ■

Lema A.2. *Seja A um anel principal. Então todo elemento não inversível $a \in A$ tem um divisor irredutível nesse anel.*

Demonstração: Se $a = 0$, a demonstração é imediata. Caso contrário, considere o ideal $I_0 =< a >$. Se esse ideal for maximal, então, devido à Proposição A.5, a é irredutível.
Se I_0 não for maximal, então existe um ideal $I_1 =< a_1 >$ em A, diferente de A, que contém propriamente I_0. Ou seja, $I_0 \subset I_1$, $I_0 \neq I_1$ e $I_1 \neq A$. Se I_1 for maximal, então a_1 é irredutível. Mas, como $< a > \subset < a_1 >$, então $a_1 \mid a$. Neste caso, a_1 é um divisor de a.
Se I_1 não for maximal, repete-se o raciocínio, o que levará à conclusão de que existe um ideal $I_2 =< a_2 >$ em A, diferente de A. tal que $< a_1 > \subset < a_2 >$, $I_2 \neq I_1$. De novo, temos pela frente as mesmas duas possibilidades: ou I_2 é maximal e a_2 é um elemento irredutível que divide a_1, e, portanto, também a, ou I_2 não é maximal.
Mas devido ao Lema A.1, nenhuma sequência $I_0 \subset I_1 \subset I_2 \subset \cdots$ de ideais em A pode ser estritamente crescente. Logo, para um índice $r + 1$ o ideal $I_{r+1} =< a_{r+1} >$ será maximal; o elemento a_{r+1} assim obtido é irredutível e divisor de $a_r, a_{r-1}, \cdots, a_1, a$ ■

Proposição A.6. *Todo anel principal é fatorial. Isto é, se A é um anel principal, então todo elemento $a \in A$, não nulo e não inversível, pode ser decomposto em um produto de fatores irredutíveis. Além disso, duas decomposições em fatores irredutíveis, do mesmo elemento não nulo e não inversível, têm igual número de fatores e cada fator de uma delas é associado de algum fator da outra.*

Demonstração: Pela Proposição A.4, temos que a condição (2)' do Teorema A.1 é satisfeita. Então precisamos apenas mostrar a existência da decomposição de fatores irredutíveis em um anel principal.

Se $a \in$ A é irredutível, não há nada a demonstrar. Então suponhamos a redutível. Devido ao Lema A.2, a tem um divisor irredutível $p_1 \in A$, o que garante a existência de $a_1 \in A$ ($a_1 \neq 0$, a_1 não inversível) tal que $a = p_1 a_1$. Se o fator a_1 for irredutível, a demonstração está encerrada. Caso contrário, repete-se o raciocínio com a_1, e assim se chegará a uma igualdade $a_1 = p_2 a_2$, em que os fatores estão em A e p_2 é irredutível. Nesta altura, $a = p_1 p_2 a_2$. Se a_2 for irredutível, a demonstração está encerrada. Caso contrário, repete-se o raciocínio com a_2, e assim por diante. Como a alternativa "a_j não é irredutível"não pode se repetir indefinidamente, em função do Lema A.1. Então, numa dada etapa do raciocínio, $a_s = p_s$ é irredutível e, portanto:

$$a = p_1 p_2 \cdots p_s$$

em que todos os fatores são irredutíveis. ■

A.6 Anéis euclidianos

Estudaremos certos anéis que admitem um algorítmo de divisão análogo à divisão de anel $\mathbb{Z}$ dos números inteiros.

Definição A.10. *Dizemos que um anel de integridade A é anel ϕ-euclidiano se existir uma função $\phi : A \setminus \{0\} \to \mathbb{N}$ tal que:*

(i) Dados a e $b \in A \setminus \{0\}$, então $\phi(ab) \geq \phi(a)$.

(ii) Se a e $b \in A$ e $b \neq 0$, então existem q e r em A, tais que $a = bq + r$ com $r = 0$ ou $\phi(r) < \phi(a)$.

Proposição A.7. *Todo anel ϕ-euclidiano é principal, e portanto fatorial.*

Demonstração: Seja A um anel ϕ-euclidiano e seja $I \neq \{0\}$ um ideal de A. O conjunto $\{\phi(a) \in \mathbb{N};\ a \in I \ e \ a \neq 0\}$ é não vazio, logo, este conjunto tem mínimo $\phi(b)$, com $b \in I$ e temos $< b > \subseteq I$. Se x é um elemento qualquer de I, então existem elementos q e r em A tais que $x = qb + r$, onde $\phi(r) < \phi(b)$ se $r \neq 0$; notando-se que $r = x - qb \in I$ e então $r \in I$. Como, dada a escolha de b, a alternativa $r \neq 0$ não pode ocorrer, então $x - bq = 0$, $x = bq$ e, portanto, $x \in < b >$ ■

Referências

[1] DOMINGUES, H.H. e IEZZI, Gelson - **Álgebra Moderna**. São Paulo, Atual, 2003.

[2] ENDLER, O. - **Teoria dos Números Algébricos**. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 2006.

[3] ENGLER, A. J. e BRUMATI, P. - **Inteiros Quadráticos e o Grupo de Classes**. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 2001.

[4] GONÇALVES, A. - **Introdução à Álgebra**. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 2006.

[5] MONTEIRO, L. H. J. - **Elementos de Álgebra**. Rio de Janeiro, Livros Técnico e Científicos Editora, 1978.

[6] RIBEMBOIM, P. - **Algebraic Numbers**. Ontorio, Wiley-Interscience, 1972.

[7] SAMUEL, P. - **Algebraic Theory of Numbers**. Londres, Kershaw Publishing Company LTD, 1971 (Tradução do original francês: Théorie algébrique des nombres. Paris, Hermann, 1967).

[8] STEWART, I. e Tall, D. - **Algebraic Number and Fermat's Last Theorem**. Massachusetts, A K Peters, 2002.