Universidade Federal Rural de Pernambuco

Departamento de Matemática
Monografia em Matemática

Domínios com Fatoração Única em Ideais

Matheus Nunes Soares

Recife – PE
Dezembro 2018

Matheus Nunes Soares

Domínios com Fatoração Única em Ideais

Trabalho de Conclusão de Curso apresentado à Coordenação de Curso de Licenciatura em Matemática da Universidade Federal Rural de Pernambuco como requisito para obtenção do título de Licenciado em Matemática.
Orientador: Prof. Dr. Gabriel Araújo Guedes

Recife – PE
Dezembro de 2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

S676d Soares, Matheus Nunes.
Domínios com fatoração única em ideais / Matheus Nunes Soares. – Recife, 2018.
51 f.

Orientador(a): Gabriel Guedes Araújo.
Trabalho de Conclusão de Curso (Graduação) – Universidade Federal Rural de Pernambuco, Departamento de Matemática, Recife, BR-PE, 2019.
Inclui referências.

1. Matemática 2. Anéis 3. Ideais 4. DFU 5. DIP 6. Dedekind I. Araújo, Gabriel Guedes, orient. II. Título

CDD 510.7

Domínios com Fatoração Única em Ideais

Trabalho de Conclusão de Curso apresentado à Coordenação de Curso de Licenciatura em Matemática da Universidade Federal Rural de Pernambuco como requisito para obtenção do título de Licenciada em Matemática.

Orientador: Prof. Dr. Gabriel Araújo Guedes

Aprovado em: ____ / ____ / ____

COMISSÃO EXAMINADORA:

Prof. Dr. Gabriel Araújo Guedes – UFRPE

Prof. Me. Danilo da Nóbrega Santos – UFRPE

Prof. Me. Tiago Duque Marques – UFRPE

Agradecimentos

Primeiramente, quero agradecer aos meus pais por acreditarem em mim, me auxiliarem em tudo que fora necessário e por serem as primeiras pessoas a me ensinarem sobre a vida.

Gostaria de agradecer a minha esposa, Gleyce Kelly, por estar comigo em todos os momentos e me ajudar sempre que necessário. Você é uma das pessoas mais importantes na minha vida.

Agradeço muitíssimo ao professor Thiago Dias (DK) por todas as dicas e puxões de orelhas que fortaleceram meu crescimento acadêmico. Parte de tudo que dá certo em minha vida acadêmica eu dedico ao Sr.

Agradeço ao meu orientador, Gabriel Guedes, por todo o auxílio e disposição em fazer com que esse trabalho desse certo. Também agradeço pelas Pizzas.

Agradeço a professora Thamires por ter me dado suporte em basicamente tudo durante toda a minha graduação.

Agradeço também ao professor Gilson por ter me auxiliado durante meus dois últimos períodos da graduação.

Agradeço ao Bar Rainha da Sucata por motivos óbvios.

Agradeço em especial à Xandy, Vital, Lenin(fala muito alto) e Sobral, pelo café de tarde na tia da barraca, por jogar xadrez, pela tiração de onda, pela companhia no R.U e por toda amizade que vocês me deram.

Agradeço à Arcasa (Shadownildo), Arthur (Gordo), Caio (Caio), Gabriel (Lass), e Luiz (nick?) pela amizade que dura até hoje, mesmo cada um morando em uma ponta do Brasil, pelas discussões sobre todo tipo de assunto, pelas risadas nos jogos e por serem vocês.

Resumo

O trabalho a seguir é um estudo de domínios de integridade que não são domínio de fatoração única, entretanto são domínios de Dedekind. Em outras palavras, os elementos do conjunto não possuem fatoração únicas, mas os seus ideais possuem. O principal objetivo do trabalho é verificar que o anel dos inteiros quadráticos $\mathbb{Z}[\sqrt{-5}]$ é um domínio de Dedekind mas não é DFU.

Palavras-chave: DFU, ideais, aneis.

Abstract

The following work is a study on integral domains that are not UFD, but are Dedekind Domains, in other words, the elements of the domain do not have unique factoration but your ideals have it. The principal objective is proof that the quadratic ring $\mathbb{Z}[\sqrt{-5}]$ is Dedekind domains but not UFD.

Keywords: UFD, ideals, rings.

Sumário

Introdução

No final do século XIX o matemático alemão Richard Dedekind iniciou o estudo do conjunto dos polinômios como uma estrutura algébrica. Dedekind introduziu a nomenclatura e o estudo dos *ideais* e dos *módulos*. Nesse sentido, tais estruturas serão definidas no decorrer do trabalho, entretanto, vale aqui salientar que em nenhuma de suas anotações, o autor utilizou a nomenclatura *anel*.

Em 1982, David Hilbert introduz a nomenclatura de *anel* que, em alemão, possui o significado de associação. Entretanto, segundo Harvey Couhn em seu livro *Advanced number theory*, (1980) o real motivo de Hilbert ter escolhido o nome "anel"para estas estruturas decorreu de suas observações, onde ele percebeu que havia um efeito cíclico em potências de determinados elementos.

A partir disso, definimos os anéis como estruturas algébricas que satisfazem seis propriedades. Além disso, adicionando mais algumas propriedades nós teremos os domínios.

Durante os anos iniciais nas escolas, os alunos são ensinados acerca da fatoração dos números inteiros. Mais a frente, durante os primeiros anos de graduação, os alunos aprendem que esta fatoração pode ser generalizada para outros domínios. Naturalmente, podemos nos indagar sobre a generalização da fatoração, não nos restringindo apenas à elementos.

Neste sentido, o objetivo deste trabalho é estudar sobre domínios que seus elementos não são fatorados de maneira únicas, mas seus ideais são, ou seja, os Domínios de Dedekind. Para isso, construiremos toda argumentação a partir do domínio $\mathbb{Z}[\sqrt{-5}]$. É fundamentado metodologicamente através da pesquisa bibliográfica de fontes secundárias. Assim como apontado por Marconi e Lakatus, (1985), toda pesquisa implica em um levantamento de dados de diversas fontes que servem como suporte para desenvolvimento dos temas trabalhados, recolhendo informações prévias sobre eles. Nesse sentido, ainda segundo as autoras, o modelo escolhido de documentação indireta bibliográfica se caracteriza por

tomar conhecimento das bibliografias relacionadas ao tema estudado, com objetivo de analisar os materiais escritos e publicados que propiciam o exame do assunto sob novos enfoques com conclusões distintas das anteriores.

Capítulo 0

Conceitos prévios necessários

Antes de falarmos propriamente do que estamos propondo, precisamos definir alguns conceitos prévios e notações que serão utilizados ao decorrer deste trabalho. Para compreender o que será apresentado, é necessário que o leitor tenha um conhecimento prévio sobre resultados básicos de teoria dos números.
A primeira estrutura que precisamos definir e será utilizada ao longo de todo trabalho é o *Anel*.

Definição 1. Um conjunto A munido de duas operações $+, \cdot$ (usualmente chamadas de soma e produto) é dito um anel se para todo $a, b, c \in (A, +, \cdot)$:

1. $(a + b) + c = a + (b + c)$;

2. $a + b = b + a$;

3. $\exists\ 0_A \in (A, +, \cdot)$ tal que $a + 0 = a$;

4. $\forall\ a \in A\ \exists\ (-a) \in (A, +, \cdot)$ tal que $a + (-a) = 0$;

5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

6. $a \cdot (b + c) = a \cdot b + a \cdot c$;

7. $(b + c) \cdot a = b \cdot a + c \cdot b$.

Se o anel $(A, +, \cdot)$ satisfaz a propriedade adicional abaixo, diremos que $(A, +, \cdot)$ é um anel com identidade.

8 $\exists\ 1_A \in (A, +, \cdot)$ tal que $1_A \cdot a = a$;

Se o anel $(A, +, \cdot)$ satisfaz comutatividade do produto, diremos que $(A, +, \cdot)$ é um anel comutativo.

As propriedades acima são chamadas de *Axiomas de Anel*. Alguns textos da literatura utilizam a notação $(A, +, \cdot)$ para denotar o anel. Ao longo do trabalho, iremos utilizar apenas anéis com soma e produto usuais, logo, é a notação utilizada para anel será apenas do conjunto em questão. Ou seja, quando falarmos do *anel* A, estaremos nos referindo à *anel* $(A, +, \cdot)$. Além disso, em determinados momentos, omitiremos o "ponto"da operação do produto, utilizando apenas ab para se referir à $a \cdot b$.

Durante o texto, o termo anel estará se referindo à um anel comutativo e com identidade.

Naturalmente, após definir uma estrutura algébrica, definimos também as suas subestruturas. A primeira subestrutura que iremos definir é o *Subanel*.

Definição 2. Diremos que um subconjunto $B \subset A$ é um subanel de A, se com as operações de A, o subconjunto B satisfazer todas as propriedades de anel.

De maneira geral, é exaustivo verificar todas as 8 propriedades de anéis para um subconjunto. A caracterização a seguir facilita identificar subanéis reduzindo a necessidade de verificar todas axiomas à verificar 3 condições.

Teorema 1. *Um subconjunto $B \subset A$ é um subanel de A se para todo $a, b \in B$ as propriedades abaixo são satisfeitas:*

1. $0_A \in A$
2. $a + b \in A$
3. $a \cdot b \in A$

Um caso especial de subanéis e que será muito utilizado do início ao fim deste trabalho, são os ideais.

Definição 3. Diremos que $I \subset A$ é um ideal de A se as seguintes propriedades são satisfeitas para todo $r, s \in I$ e $a \in A$

1. $0_A \in A$
2. $r + s \in A$

3. $r \cdot a \in A$

Considere A um anel. Dados $a, b \in A$, diremos que $a|b$ (lê-se a divide b) se $b = ac, c \in A$. Além disso, um elemento $u \in A$ é dito unidade de A se existe $v \in A$ tal que $uv = 1_A$ e 1_A denota a identidade do anel.

Exemplo 1. Em $\mathbb{Z}$ as únicas unidades são 1 e -1.

Exemplo 2. Se $\mathbb{K}$ é um corpo, então as unidades do anel de polinômios $\mathbb{K}[x]$ são os polinômios constantes não nulos.

Exemplo 3. Em $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ o elemento $1 + \sqrt{2}$ é uma unidade pois

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

Além disso, $\mathbb{Z}[\sqrt{2}]$ é um exemplo de anel com infinitas unidades.

Observação: Dado $u \in A$ uma unidade com inversa v. Então, para qualquer elemento $a \in A$ temos que $u(vb) = (uv)b = b$. Em outras palavras, a unidade divide todos os elementos de A.
Além disso, dizemos que um elemento a é associado à b se $a = bu$, onde u é uma unidade. Consequentemente, a está associado à b se, e somente se, b está associado à a.

Definição 4. Um elemento não-nulo $p \in \mathcal{R}$ é dito irredutível se p é não-unidade e os únicos divisores de p são os associados e as unidades de $\mathcal{R}$.

Definição 5. Um elemento não-nulo $p \in \mathcal{R}$ é dito primo se as seguintes condições são verdadeiras:

a) p é não-unidade.

b) se $p|ab$, então $p|a$ ou $p|b$.

Definição 6. Diremos que um polinômio p é mônico se o coeficiente do termo de grau líder é igual à 1.

Exemplo 4. $p(x) = x^2 + 1$; $q(t) = t^n + t^{n-1} + t^{n-2} + \ldots + t$ são polinômios mônicos.

Definição 7. Diremos que K é uma extensão do corpo F, se K é um subcorpo de F. Em geral, utilizaremos a notação K/F

Definição 8. A característica de um corpo é o número inteiro positivo n tal que $\overbrace{1 + 1 + 1 + .. + 1}^{n-vezes} = 0$.

Capítulo 1

Domínios

1.1 Domínio de Integridade

Definição 9. Diremos que um conjunto $\mathcal{A}$ é um Domínio de Integridade se:

i) $\mathcal{A}$ é um anel;

ii) $\mathcal{A}$ é comutativo;

iii) $\exists\ 1_{\mathcal{A}} \in \mathcal{A}$ tal que $\forall x \in \mathcal{A}$, $1_{\mathcal{A}} x = x 1_{\mathcal{A}} = x$;

iv) $\forall x, y \in \mathcal{A}$ não-nulos, $xy = 0$ implica que $x = 0$ ou $y = 0$.

Teorema 2. *Se p é um elemento não-nulo e não-unidade em um domínio de integridade $\mathcal{R}$, então p é irredutível se, e somente se, ocorre a seguinte implicação:*

$$\textit{se } p = rs\textit{, então } r \textit{ ou } s \textit{ é uma unidade.}$$

Demonstração. Se p é irredutível, então r é um divisor de p. Pela definição, r é uma unidade ou r é um associado de p. Se r é uma unidade, a proposição segue. Se r é associado, então $r = pv$, logo, $p = rs = pvs$. Cancelando p, temos que $1 = vs$. Então, s é uma unidade.

Para provar a volta, suponha que p tenha a implicação citada. Seja c um divisor qualquer de p, chame $p = cd$. Pela hipótese, c ou d é uma unidade. Se d for uma unidade, multiplique ambos os lados por d^{-1}. Logo, $c = d^{-1}$. Logo, ou c é uma unidade ou c é um associado de p. ■

Definição 10. Um domínio de integridade $\mathcal{R}$ é dito Domínio Euclidiano se existe uma função δ de elementos não-nulo de $\mathcal{R}$ em elementos inteiros não-negativos com a seguinte propriedade:

i) Se a e b são elementos não-nulos de R, então $\delta(a) \leq \delta(ab)$

ii) Se $a, b \in \mathcal{R}$ e $b \neq 0_R$ então existem $q, r \in R$ tal que

$a = bq + r$ e, ou $r = 0_R$ ou $\delta(r) < \delta(b)$.

Exemplo 5. Se F é um corpo, então o domínio dos polinômios $F[x]$ é um domínio com a função $\delta(f(x)) = \deg(f(x))$

Exemplo 6. O anel dos inteiros Gaussianos, $\mathbb{Z}[i]$, com $\delta(a + bi) = a^2 + b^2$.

Teorema 3. *Seja $\mathcal{R}$ um Domínio Euclidiano e u um elemento não-nulo. As seguintes condições são equivalentes:*

i) *u é uma unidade.*

ii) $\delta(u) = \delta(1_R)$.

iii) $\delta(c) = \delta(uc)$, *c nãonulo.*

Demonstração. **(1)** $\implies$ **(2)** Suponha que u é uma unidade. Logo, $\delta(u) = \delta(u1_R) \leq \delta(1_R)$ e $\delta(1_R) = \delta(uu^{-1}) \leq \delta(u(uu^{-1})) = \delta(u)$. Portanto, $\delta(u) = \delta(1_R)$.

(2) $\implies$ **(3)** Tome $c \in R$ e u uma unidade. Logo, $\delta(c) \leq \delta(uc)$. Além disso, $\delta(c) = \delta(cuu^{-1}) \geq \delta(uc)$. Portanto, $\delta(uc) = \delta(c)$.

(3) $\implies$ **(1)**

Pela segunda propriedade de Domínio Euclidiano, podemos escrever $c = (uc)q + r$. Portanto,

$$\delta(c) \leq \delta(c(1_R - uq)) = \delta(c - ucq) = \delta(r) < \delta(uc) = \delta(c).$$

Logo, temos uma contradição. Então, $r = 0_R$. Portanto, $c = (uc)q$ que implica que u é uma unidade. ■

Definição 11. Seja $\mathcal{R}$ um Domínio Euclidiano e $a, b \in R$ (não-nulos). O Máximo Divisor Comum, que denotaremos como mdc, de a e b é um elemento d tal que:

i) $d|a$ *e* $d|b$

ii) *Se* $c|a$ *e* $c|b$ *então* $\delta(c) \leq \delta(d)$

Teorema 4. *Seja $\mathcal{R}$ um Domínio Euclidiano e $a, b \in R$ então:*

i) *Se d é um mdc de a e b então todo associado de d também é um mdc;*

ii) *Quaisquer dois mdcs são associados;*

iii) *Se d é um mdc de a e b então existem $u, v \in R$ tal que $d = au + bv$.*

Demonstração. Seja $S = \{\delta(w) \mid 0_R \neq w \in R \text{ e } w = as + bt \text{ para certos } s, t \in R\}$. Desde que $a = a1_R + b0_R$ e $b = a0_R + b1_R$ é não-nulo, S é o conjunto não-vazio de inteiros não-negativos. Pelo axioma da boa ordem, S contém um elemento mínimo, ou seja, há elementos $d^*, u^*, v^* \in R$ tal que $d^* = au^* + bv^*$ e para todo elemento não-nulo w de forma $as + bt$, $\delta(d^*) \leq \delta(w)$. Queremos que d^* seja um mdc de a e b. Como $\mathcal{R}$ é um Domínio Euclidiano, então existem q e r tal que $a = d^*q + r$ e, ou $r = 0_R$ ou $\delta(r) < \delta(d^*)$. Note que

$$r = a - d^*q = a - (au^* + bv^*)q = a(1_R - qu^*) + b(-v^*q).$$

Como r é uma combinação linear de a e b então não podemos ter $\delta(r) < \delta(d^*)$. Então, $d^*|a$ (Argumento análogo para d^* divide b). Portanto, d^* é um divisor comum de a e b. Seja c outro divisor comum de a e b. Então, $a = cs$ e $b = ct$ para certos $s, t \in R$ e portanto

$$d^* = au^* + bv^* = c(su^* + tv^*).$$

Logo, $\delta(c) \leq \delta(c(su^* + tv^*)) = \delta(d^*)$. Concluímos que d^* é um mdc de a e b, uma vez que todo divisor comum c de a e b divide d^*. ■

Corolário 5. *Se $\mathcal{R}$ é um Domínio Euclidiano e $a, b \in R$. Então d é o mdc de a e b se, e somente se, d satisfaz as seguintes condições:*

i) $d|a$ e $d|b$;

ii) se $c|a$ e $c|b$ então $c|d$.

Demonstração. Se $d = mdc(a, b)$, então por definição d satisfaz a propriedade (i). Além disso, como $c|a$ e $c|b$ então c é um divisor comum de a e b. Dado que d é o máximo divisor comum, temos que $c|d$, mostrando assim a propriedade (ii) Por outro lado, suponha que (i) e (ii) ocorrem. Por (ii) sabemos que todo divisor c divide d, portanto, d é o máximo divisor comum.

■

Observação: Elementos a e b são ditos primos relativos ou coprimos se $mdc(a, b) = 1_{\mathcal{R}}$.

Teorema 6. *Seja $\mathcal{R}$ é um Domínio Euclidiano e $a, b, c \in R$. Se $a|bc$ e a e b são primos relativos, então $a|b$.*

Corolário 7. *Seja p um elemento irredutível em um Domínio Euclidiano R.*

i) Se $p|bc$, então $p|b$ ou $p|c$ ii) Se $p|a_1...a_m$ então p divide cada um dos a_i

Teorema 8. *Seja $\mathcal{R}$ um Domínio Euclidiano no qual todo elemento não-nulo e não-unidade de $\mathcal{R}$ é um produto de elementos irredutíveis, então:*
Se $p_1..p_r = q_1...q_s$ então $r = s$ e (depois de uma reorganização, se necessário) p_i é associado à q_i

Definição 12. Um ideal I é dito principal quando todo conjunto de geradores de I pode ser reduzido à um único elemento. Em outras palavras,

$$I = (a_1, ..., a_n) = (a).$$

1.2 Domínio de Ideais Principais (DIP)

Definição 13. Chamaremos de Domínio de Ideias Principais o Domínio de Integridade onde todo ideal é principal.
Antes de exemplificar a ideia de DIP, enunciaremos um teorema que permitirá a caracterização desses Domínios de Integridades especiais.

Teorema 9. *Todo Domínio Euclidiano é um DIP.*

Demonstração. Seja A um Domínio Euclidiano. Suponha que I é um ideal não-nulo A. Então, existem um conjunto $C = \{\delta(i) \mid i \in I\}$ de inteiros não-negativos. Pelo Princípio da Boa-Ordem, existe um menor elemento em C. Em outra palavras, existe $b \in I$ tal que $\delta(b) \leq \delta(i)\ \forall i \in I$. Como I é ideal e $b \in I$ então $rb \in I$ e, portanto, $(b) \subset I$. Reciprocamente, se $c \in I$ então existe $k, r \in A$ tais que

$$c = kb + r,\ com\ \delta(r) < \delta(k)\ ou\ r = 0_R$$

Manipulando a equação acima, temos que $r = c - bk$. Como $bk \in I$ e $c \in I$ então $r \in I$, basta observar a caracterização resultou em um ideal. Consequentemente, $\delta(r) \not< \delta(b)$. Reciprocamente, se $r = 0_R$ então $c = bk \in (b)$. Logo, $I \subset (b)$. Portanto, concluímos que $I = (b)$. Logo A é um DIP. ■

Por outro lado, a recíproca deste teorema não é válida. Iremos mostrar um exemplo para essa afirmação mais a frente pois há a necessidade de definir algumas notações previamente.

Proposição 10. *Sejam a e b elementos em um domínio de integridade A. Então*

(1) $(a) \subseteq (b)$ *se, e somente se,* $b|a$*;*

(2) $(a) = (b)$ *se, e somente se,* $a|b$ *e* $b|a$*;*

(3) $(a) \subsetneq (b)$ *se, e somente se,* $b|a$ *e* b *não é associado à* a*.*

Demonstração. (1) Se $(a) \subseteq (b)$, então dado $a \in (a)$, temos que $a \in (b)$, como todo elemento em (b) é da forma br, com $r \in A$, temos que $a = br_0$ para certo $r_0 \in A$ e, portanto, $b|a$.

Por (1) temos que $(a) \subseteq (b)$ se, e somente se, $b|a$, consequentemente, $(b) \subseteq (a)$ se, e somente se, $a|b$, juntando ambas temos a equivalência (2).

Para demonstrar (3) utilizaremos (1), (2). Note que $a|b$ *e* $b|a$ se, e somente se, a é associado à b, pois, se $a|b$ e $b|a$, então:

$$a = bc \text{ e } b = ad, \quad \text{para certos c,d} \in \text{A}.$$

Logo, $a = adc$. Portanto, c é uma unidade. Logo, a é associado a b. Além disso, se a é associado a b, então $a = ub$ onde u é uma unidade, portanto $b|a$. Por outro lado, $b = au^{-1}$, logo $a|b$.

Negando a bicondicional temos que $a \nmid b$ ou $b \nmid a$ se, e somente se, a não é associado à b. Para a ida, basta perceber que como $(b) \nsubseteq (a)$, então $a \nmid b$. Logo, temos que $(a) \neq (b)$ consequentemente $a \nmid b$ ou $b \nmid a$. Independente de qual caso aconteça, a não é associado à b. ■

Como motivação da próxima definição pensaremos no seguinte fato: Dado um elemento a_1 (que admita fatoração), então podemos escrever a_1=p_1a_2 onde p_i, $i = 1, ..., n$ são primos. Suponha que podemos repetir o processo (agora para a_2), então $a_1 = p_1p_2a_3$. Entretanto, se reduzirmos de modo que em certo n, $a_n = p_n$ seja primo, e esse argumento pode ser utilizado por conta do Teorema Fundamental da Aritmética, então a decomposição resultará em $a_n = p_1 * ... * p_n$. Consequentemente, como p_n é primo, as próximas decomposições serão $a_n = p_1 * ... * p_n * 1$, $a_n = p_1 * ... * p_n * 1 * 1$, $a_n = p_1 * ... * p_n * 1 * 1 * ...$. Logo, a decomposição se estabiliza em determinado momento. Mediante a isso, faz sentido questionarmos se há uma analogia para ideais principais.

Definição 14. Um domínio de integridade satisfaz $\mathcal{R}$ a condição de cadeias ascendentes

de ideias se dada uma cadeia $(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$, então existe um n índice de (a_i) onde a cadeia estabiliza. Ou seja, $(a_n) = (a_i)\ \forall\ i \geq n$.

Lema 11. *Todo DIP satisfaz a Condição de Cadeias Ascendentes.*

Demonstração. Considere $(a_1) \subseteq (a_2) \subseteq \ldots$ uma cadeia ascendente de ideais em um DIP que denotaremos por $\mathcal{R}$. Seja A o conjunto $\bigcup_{i\geq 1}(a_i)$. Verificaremos se A é um ideal. Suponha que $j \leq k$ e $a \in (a_j)$ e $b \in (a_k)$. Como $\mathcal{R}$ satisfaz a CCA, temos que $(a_j) \subseteq (a_k)$. Logo, a e b pertencem à (a_k). Como (a_k) é um ideal, então $a - b \in (a_k)$ e $ra \in (a_k) \subseteq A$. Portanto, A é um ideal. Como $\mathcal{R}$ é um DIP, então $A = (c)$ para certo c em $\mathcal{R}$. Como $A = \bigcup_{i\geq 1}(a_i)$ então $c \in (a_n)$ para certo n. Logo, $qc \in (a_n)$, com $q \in R$ pois (a_n) é um ideal. Como os elementos de (c) são da forma qc, então $(c) \in (a_n)$. Portanto, $(c) = A = (a_n)$. Concluí-se que $(a_i) = (a_n)$ para todo $i \geq n$ ■

Lema 12. *Seja $\mathcal{R}$ um DIP. Se p é irredutível em $\mathcal{R}$ e $p|bc$ então $p|b$ ou $p|c$.*

Demonstração. Se $p|bc$ então $pk = bc$. Logo, $bc \in (p)$. Se concluirmos que (p) é um ideal primo, então o Lema está provado, já que em um anel comutativo todo ideal maximal é primo e nosso anel é comutativo pois estamos em um domínio de integridade. Faremos do modo clássico, suponha que I é um ideal tal que $(p) \subseteq I \subseteq R$. Como $\mathcal{R}$ é um DIP, então $I = (a)$ para certo a em $\mathcal{R}$. Logo, $(p) \subseteq (a)$. Portanto, $p|a$, entretanto, p é irredutível por hipótese, então a é associado à p ou $p = 1_R$. Se $a = 1_{\mathcal{R}}$, então $(a) = \mathcal{R}$ e (p) é maximal. Por outro lado, se a é associado à p, então p também é associado à a. Logo $au = p$, que implica que $a|p$. Logo $a \in (p)$ e como (p) é ideal, $(a) \subseteq (p)$. Portanto, $(a) \subseteq (p) \subseteq (a)$. De qualquer modo, $(a) = (p)$. Concluindo assim a demonstração. ■

Definição 15. Diremos que um anel $\mathcal{R}$ é *Noetheriano* se todo ideal $\mathcal{I} \subseteq \mathcal{R}$ é finitamente gerado.

Os anéis com essa propriedade receberam esse nome em homenagem a matemática alemã Emmy Noether.

Teorema 13. *$\mathbb{Z}[x]$ é Noetheriano.*

Para verificar tal afirmação, utilizaremos o Teorema da base de Hilbert.
Um resultado interessante e que será útil para conclusão do nosso trabalho é que $\mathbb{Z}[x]$ é Noetheriano. Este resultado decorre imediatamente do Teorema da Base de Hilbert, o qual demonstraremos a seguir.

Teorema 14. *Se R é um anel Noetheriano, então $R[x]$ é Noetheriano.*

Demonstração. Suponha que $I \subseteq R[x]$ seja um ideal não-finitamente gerado. Logo, por recorrência, existe uma sequência $\{f_0, f_1, f_2, \ldots, f_n, \ldots\}$ de polinômios de $R[x]$ tal que se J_n é um ideal finitamente gerado por $f_0, \ldots, f_{n-1}$, então $f_n \in I - J_n$ tem grau mínimo. Note que $\{deg(f_0), deg(f_1), \ldots, deg(f_n), \ldots\}$ é uma sequência não-decrescente de números inteiros positivos. Seja a_n o coeficiente líder do polinômio f_n e seja $J \subseteq R$ gerado por $a_0, a_1, \ldots, a_n, \ldots$. Como R é Noetheriano, então

$$(a_0) \subset (a_0, a_1) \subset (a_0, a_1, a_2) \subset \ldots$$

estabiliza em certo n_0. Logo, $J = (a_0, \ldots, a_{n_0-1})$. Em particular,

$$a_{n_0} = \sum_{i=0}^{n_0-1} \alpha_i a_i$$

Agora, considere o polinômio

$$q(x) = \sum_{i=0}^{n_0-1} \alpha_i x^{deg(f_{n_0})-deg(f_i)} f_i$$

onde o termo líder de q é igual ao do polinômio f_{n_0}. Note que $q \in J_{n_0}$. Por outro lado, $f_{n_0} \notin J_{n_0}$, ou seja $f_{n_0} - q \in I - J_{n_0}$ tem grau menor que f_{n_0} que contradiz a minimalidade deste polinômio. ■

Teorema 15. *Se $\mathcal{R}$ é um anel Noetheriano e $\mathcal{I}$ é um ideal, então $\frac{\mathcal{R}}{\mathcal{I}}$ é noetheriano.*

1.3 Domínio de Fatoração Única (DFU)

Definição 16. Um Domínio de Integridade $\mathcal{R}$ é um DFU se todo elemento não-nulo e não-unidade de $\mathcal{R}$ é o produto de elementos irredutíveis e a fatoração é única a menos de associados. Isto é, se $p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ com cada p_i e q_j então $r = s$ e $p_i = q_i$ com $i = 1, \ldots, r$.

Observação: Em alguns casos, faz-se necessário uma reordenação dos p_i e dos q_i para que a igualdade ocorra.

Exemplo 7. $\mathbb{Z}[\sqrt{-3}]$ não é um DFU, pois

$$(1+\sqrt{-3})(1-\sqrt{-3}) = 4 = (2)(2)$$

Como o elemento 4 possui duas fatorações distintas, $\mathbb{Z}[\sqrt{-3}]$ não é um DFU.

Teorema 16. *Se a e b são elementos não nulo em um DFU que detonaremos por $\mathcal{R}$, então existe unidades u e v e irredutíveis $p_1, p_2, \ldots, p_k$ não-associados dois a dois, tais que,*

$$a = up_1^{m_1}p_2^{m_2}\ldots p_k^{m_k} \text{ e } b = vp_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$$

onde cada m_i e n_i são inteiros não-negativos. Além disso,

$$c|d \text{ se e somente se } m_i \leq n_i \text{ para cada } i = 1, 2, \ldots, k.$$

Demonstração. Supomos inicialmente que $\mathcal{R}$ é um DFU, então a e b podem ser fatorados em produto de irredutíveis. Escreveremos $a = q_1q_2\ldots q_s$ e $b = r_1r_2\ldots r_l$. Dos elementos $q_1, q_2, \ldots, q_s, r_1, r_2, \ldots, r_l$, remova todos os associados. Os q_i e r_j restantes, denote por $p_1, p_2, \ldots, p_k$. Note que cada p_i é irredutível e que não há associados dois a dois. Cada q e cada r é associado à um certo p_i. Portanto, podemos escrever $a = q_1q_2\ldots q_s$ como $a = (u_1u_2\ldots u_s)(p_1p_2\ldots p_s)$, onde os u_j são unidades de $\mathcal{R}$ ■

Corolário 17. *Todo DFU satisfaz a condição de cadeias ascendentes em ideais principais.*

Demonstração. Suponha que (a) e (b) sejam ideais principais em um DFU tal que $(b) \subsetneq (a)$. A partir disso sabemos que $a|b$ mas b não é associado à a e isso decorre de 10. Além disso por 16, $a|b$ se, e somente se, $m_i \leq n_i$. Note que se $m_i = n_i$, então $au = bv$, consequentemente b é associado à a, o que não é possível já que $(b) \subsetneq (a)$. Logo, a desigualdade é estrita, ou seja, há um certo índice j tal que $m_j < n_j$.

Suponha que $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots$ é uma cadeia de ideais principais em $\mathcal{R}$. Ainda por 10, temos que $a_i|a_1$. Suponha que $a_1 = up_1{}^{n_1}p_2{}^{n_2}\ldots p_k{}^{n_k}$ e os demais a_i são da forma $a_i = up_1{}^{m_1}p_2{}^{m_2}\ldots p_k{}^{m_k}$. Desde que haja um número finito de (a_i) a partir de certo i a inclusão se estabiliza e vira uma igualdade. Note que não pode haver um número infinito de inclusões estritas pois como para cada inclusão o expoente dos irredutíveis da decomposição de a_i decresce, em algum momento, o inteiro m_i será igual à 0. A partir disso, suponha que $a_n = up_1{}^0p_2{}^0\ldots p_k{}^0 = u$. Como u é unidade, $(a_n) = (u) = \mathcal{R}$. Pelo

modo como supomos a decomposição de cada a_i, temos que $(a_n) \subseteq a_i$. Portanto

$$(a_n) \subseteq a_i \subset \mathcal{R} = (a_n)$$

Concluímos que $(a_i) = (a_n)$. ■

Alguns resultados serão uteis ao longo desse trabalho mas apenas enunciaremos. Omitiremos a demonstração para que não fique uma leitura tão densa.

Teorema 18. *Seja p um elemento irredutível em um domínio de fatoração única $\mathcal{R}$. Se $p|bc$ então $p|b$ ou $p|c$.*

Teorema 19. *Todo DIP é um DFU.*

Demonstração. Seja $\mathcal{R}$ um domínio de ideais principais. Suponha que existe um elemento não-nulo e não-unidade $a \in \mathcal{R}$ tal que

$$q_1 q_2 \dots q_s = a = p_1 p_2 \dots p_r.$$

onde p_i e q_j são elementos irredutível em $\mathcal{R}$ e $s \geq r$. Logo, p_1 divide $q_1 \dots q_s$ e $p_1|q_j$ para certo j e p_1 primo. Reordenando os q_j podemos supor que $p_1|q_1$. Então $q_1 = u_1 p_1$, onde u_1 é uma unidade de $\mathcal{R}$, desde que q_1 e p_1 sejam irredutíveis. Logo,

$$\prod_{i=1}^{r} p_i = u_1 \prod_{j=1}^{s} q_j.$$

e

$$\prod_{i=2}^{r} p_i = u_1 \prod_{j=2}^{s} q_j.$$

Repetindo o processo até s, temos que:

$$1 = u_1 u_2 \dots u_s \prod_{j=s+1}^{s} q_j.$$

Como nenhum dos q_j é unidade, então $r = s$ e $p_1, p_2, \dots, p_r$ e $q_1, q_2, \dots, q_r$ são associados. Logo, $\mathcal{R}$ é um domínio de fatoração única. ■

1.4 Domínio de Fatoração Única que não é Domínio de Ideais Principais

A recíproca do último teorema da sessão anterior não é válida. Um exemplo para isso é que o ideal $(2, x) = \{a_n x^2 + \ldots + a_1 x + a_0 \mid a_0 \in 2\mathbb{Z} \ e \ a_1, \ldots, a_n \in \mathbb{Z}\} \subset \mathbb{Z}[x]$ não é principal. Suponha por absurdo que $(2, x)$ seja principal. Então, existe um polinômio $p(x) \in (2, x)$ tal que

$$(p(x)) = (2, x).$$

Em particular, $x \in (p(x))$ e $2 \in (p(x))$. Ou seja, podemos escrever 2 como $p(x)q(x)$ onde $q(x)$ é um elemento de $\mathbb{Z}[x]$. Logo, $p(x) = k$ para certo $k \in \mathbb{Z}$.
Além disso, por $x \in (p(x)$, logo $x = cg(x)$. Portanto, desde que $g(x) = b_n x^n + \ldots + b_1 x + b_0$, com $b_i \in \mathbb{Z}$, temos que

$$x = cb_n x^n + \ldots + cb_1 x + cb_0$$

Ou seja, $cb_1 = 1$ e $b_i = 0$ para todo $i \neq 1$. Logo, $c = \pm 1$. Entretanto, $(1) = (-1) = \mathbb{Z}[x]$. Ou seja, $(2, x) = (1) = \mathbb{Z}[x]$, que é um absurdo, já que o polinômio $1 \notin (2, x)$. Portanto, $\mathbb{Z}[x]$ não é um DIP.

Capítulo 2

Inteiros Quadráticos

2.1 Definições

Nesse capítulo, iremos introduzir um pouco de um dos alvos desse trabalho, o anel dos inteiros quadráticos. O anel $\mathbb{Z}[\sqrt{d}]$, com $d \in \mathbb{Z}$, é um tanto peculiar pois, em geral, os seus elementos não admitem fatoração única. Claro, assumiremos que $d \neq \pm 1$ e d é um inteiro livre de quadrado. Um exemplo disso já foi dado acima com o anel $\mathbb{Z}[\sqrt{-3}]$. A partir disso, iremos definir alguns conceitos necessário para os estudo dos quadráticos. Vale salientar que normalmente definimos a norma de um elemento $x \in \mathbb{Z}[\alpha]$ como $|x| = x\overline{x}$, onde $\overline{x}$ é o conjugado usual complexo.

Definição 17. Chamaremos de **Norma** a função dada por:

$$\begin{aligned} \mathcal{N} : \mathbb{Z}[\sqrt{d}] &\longrightarrow \mathbb{Z} \\ \mathbf{a + b\sqrt{d}} &\longmapsto \mathbf{a^2 - db^2} \end{aligned}$$

Exemplo 8. Considere um elemento em $\mathbb{Z}[\sqrt{2}]$, por exemplo, $2 + 3\sqrt{2}$. A norma desse elemento é $\mathcal{N}\left(2 + 3\sqrt{2}\right) = 2^2 - 2 * 3^2 = -14$.

A partir disso, faz sentido se questionar sobre a existência de resultados que envolvam os Inteiros Quadráticos e a função Norma.

Teorema 20. *Se d é um inteiro livre de quadrado, então para todo a, $b \in \mathbb{Z}[\sqrt{d}]$*

$$\mathcal{N}(x) = 0 \text{ se e somente se } x = 0 \tag{2.1}$$

$$\mathcal{N}(xy) = \mathcal{N}(x)\mathcal{N}(y). \tag{2.2}$$

Demonstração. Para mostrar (1) primeiro escreveremos x na forma dos elementos de $\mathbb{Z}[\sqrt{d}]$. Seja $x = a + b\sqrt{d}$ com $a, b \in \mathbb{Z}$. Pela definição da norma em $\mathbb{Z}[\sqrt{d}]$, temos que:

$$\mathcal{N}(x) = 0 \implies a^2 - db^2 = 0 \implies a^2 = db^2$$

Agora iremos observar dois casos. Se $d < 0$, então $db^2 \leq 0$. Mas $a^2 \geq 0$, logo a única solução da igualdade seria $a = b = 0$. Por outro lado, suponha que $a = up_1{}^{n_1} \dots p_k{}^{n_k}$ e $b = vp_1{}^{m_1} \dots p_k{}^{m_k}$. Note que cada irredutível aparece em um número par de vezes em a^2 e b^2 independende do valor de cada m_i e n_i. Além disso, d é livre de quadrados, portanto podemos escrevê-lo como

$$d = wp_1{}^{2s_1+1} \dots p_k{}^{2s_k+1}.$$

Fazendo o produto de d por b^2, teremos que cada fator irredutível aparecerá em um número ímpar de vezes, o que não é possível já que em a^2 cada p_i aparece em uma quantidade par. Portanto, a única solução é que $a = b = 0$.
Para mostrar (2) o procedimento é mais simples. Suponha que $x = a+b\sqrt{d}$ e $y = e+f\sqrt{d}$. Por definição,

$$\begin{aligned}
\mathcal{N}(xy) &= \mathcal{N}((a + b\sqrt{d})(e + f\sqrt{d}) = \mathcal{N}(ae + bfd + (af + be)\sqrt{d}) \\
&= (ae + bfd)^2 - d(af + be)^2 \\
&= a^2e^2 + b^2f^2d^2 + 2aebfd - da^2f^2 - db^2e^2 - 2dafbe \\
&= a^2(e^2 - df^2) - db^2(e^2 - df^2) = (a^2 - db^2)(e^2 - df^2) = \mathcal{N}(x)\mathcal{N}(y).
\end{aligned}$$

Concluindo assim a demonstração de (2). ■

Teorema 21. *(Teorema da Norma das Unidades) Tome d um livre de quadrado em $\mathbb{Z}$. u é unidade se, e somente se, $\mathcal{N}(u) = \pm 1$.*

Demonstração. Para mostrar a ida, tome u um elemento em $\mathbb{Z}[\sqrt{d}]$ tal que u é unidade. Como u é unidade, sabemos que existe um v em $\mathbb{Z}[\sqrt{d}]$ tal que $uv = 1$. Portanto, utilizando

o teorema anterior, $\mathcal{N}(u)\mathcal{N}(v) = \mathcal{N}(uv) = N(1) = N(1 - 0\sqrt{d}) = 1^2 - 0^2 = 1$. Já para a volta, tome $u = x + \sqrt{d}y$ e $\bar{u} = x - \sqrt{d}y$. Por definição $\mathcal{N}(u) = x^2 - dy^2 = \pm 1$, portanto $\mathcal{N}(\bar{u}) = x^2 - d(-y^2) = x^2 - dy^2 = \mathcal{N}(u) = \pm 1$. Logo,

$$u\bar{u} = (x + \sqrt{d}y)(x - \sqrt{d}y) = x^2 - \sqrt{d}y^2 = \mathcal{N}(u) = \mathcal{N}(\bar{u}) = \pm 1$$

Concluímos que $u\bar{u} = 1$ ou $u\bar{u} = -1$, ou seja, u é unidade. ■

Exemplo 9. Em $\mathbb{Z}[\sqrt{3}]$ o elemento $x = 7+4\sqrt{3}$ é uma unidade. Pois $\mathcal{N}(x) = 49-3*16 = 1$.

Teorema 22. *Se $p \in \mathbb{Z}[\sqrt{d}]$ e $\mathcal{N}(p)$ é primo, então p é irredutível.*

Demonstração. Suponha que p não é irredutível, então existem $x, y \in \mathbb{Z}[\sqrt{d}]$ irredutíveis, tais que $p = xy$. Pelo teorema 20, $\mathcal{N}(p) = \mathcal{N}(xy) = \mathcal{N}(x)N(y)$. Como x e y não são unidades, $\mathcal{N}(x) \neq 1$ e $\mathcal{N}(y) \neq 1$. Daí tem-se que independente do valor que $\mathcal{N}(x)$ e $\mathcal{N}(y)$ assumirem, seja irredutível ou não, o produto $\mathcal{N}(x)\mathcal{N}(y)$ é não-irredutível. ■

Assim como no conjunto dos números inteiros, os elementos em $\mathbb{Z}[\sqrt{d}]$, com d livre de quadrados, são fatores em produtos de irredutíveis, o que torna-os um pouco mais plausível de compreender, dada essas semelhanças o que já conhecemos. Apesar das semelhanças, para certos elementos $d \in \mathbb{Z}$ a fatoração em produtos de irredutíveis não é única, portanto não é um DFU. O exemplo abaixo deixará mais claro esta afirmação.

Exemplo 10. Em $\mathbb{Z}[\sqrt{-3}]$, o elemento 6 possui mais de uma fatoração em produto de irredutíveis, pois

$$\begin{aligned} 6 &= (2 * 3) \\ 6 &= (3 - \sqrt{-3})(3 + \sqrt{-3}) \end{aligned}$$

Não é complicado encontrar exemplos de domínios $\mathbb{Z}[\sqrt{d}]$ que não são Domínios de Fatoração Única.

Definiremos agora um conjunto que é importante para o desenvolvimento de alguns tópicos deste trabalho.

Definição 18. Sejam I e J ideais em um anel $\mathcal{R}$. Definiremos o produto dos ideais como:

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \mid n \geq 1,\ x_i \in I \ e\ y_i \in J \right\}$$

Exemplo 11. Considere o anel $\mathbb{Z}$ e os ideais $(3), (7)$. O produto dos ideais é dado por $(3)(7) = \left\{ \sum_{i=1}^{n} (3k_i)(7q_i) \mid n \geq 1,\ k_i \in I \ e\ q_i \in J \right\}$, que é o mesmo que o conjunto dos múltiplos de $3 * 7 = 21$.

2.2 Domínio de Ideais Principais que não é Euclidiano

Agora, verificaremos que nem todo domínio de ideais principais é um Domínio Euclidiano. Para isso, mostraremos que $\mathcal{A} = \mathbb{Z}[\frac{1}{2}\left(1 + \sqrt{-19}\right)]$ é um domínio de ideais principais mas não é Domínio Euclidiano. Iremos dividir a demonstração em alguns passos.
Note que $\mathcal{A}$ é um domínio de integridade, pois tomando $u = \frac{1}{2}\left(1 + \sqrt{-19}\right)$, temos que

$$u^2 = \frac{1}{4}\left(1 + 2\sqrt{-19} - 19\right)$$

$$u^2 = \frac{1}{2}\left(+10 - 10 - 9 + \sqrt{-19}\right)$$

$$u^2 = \frac{1}{2}\left(1 + \sqrt{-19}\right) - 5$$

$$u^2 = u - 5.$$

Logo, o polinômio $p(x) = x^2 - x + 5$, pelo critério de Einsentein, temos que p é irredutível. Portanto, $\mathcal{A}$ é um domínio de integridade.

Lema 23. *Em $\mathcal{A}$, as únicas unidades são 1 e -1.*

Demonstração.

$$|a + bu| = \pm 1$$

$$(a + bu)\,\overline{(a + bu))} = \pm 1$$

$$\left(a + b\left(\frac{1}{2}\left(1 + \sqrt{-19}\right)\right)\right)\left(a + b\left(\frac{1}{2}\left(1 - \sqrt{-19}\right)\right)\right) = \pm 1$$

$$a^2 + ab + 5b^2 = \pm 1$$

$$\implies \Delta = b^2 - 4(5b^2 \pm 1) = -19b^2 \pm 4$$

Note que, a única solução para que o discriminante seja positivo é que $-19(0)^2+4 = 4$. Logo, $b = 0$. Portanto, $a^2 = \pm 1$, que implica que $a = 1$. Assim, concluímos que as únicas unidades são ± 1. ■

Lema 24. *Os elementos* 2 *e* 3 *são irredutíveis em* $\mathcal{A}$.

Demonstração. Como 2 é não-unidade, segue que $\frac{1}{2} \notin \mathbb{Z}[u]$. Suponha que existem $n, m \in \mathbb{Z}[u]$ tal que $2 = nm$. Portanto, $4 = |2| = |nm| = |n||m|$. Note que, como $|n|$ e $|m|$ são números inteiros positivos, então os possíveis pares para $(|n|, |m|)$ são

$$(1, 4), (2, 2), (4, 1).$$

Pelo teorema da norma das unidades, $(1, 4), (4, 1)$ implicam em 2 ser irredutível, pois $|n| = \pm 1$ implica em n ser unidade (o mesmo vale para m). Logo, basta verificar o caso $(2, 2)$.
Tome $n = x + yu$. Logo,

$$2 = |n| = x^2 + xy + 5y^2.$$

Se olharmos como um polinômio na variável x, temos que $x^2 + xy + 5y^2 - 2 = 0$, logo $\Delta = y^2 - 20y^2 + 8 = -19y^2 + 8$. Como $y^2 \geq 0$, segue a única solução para $\Delta \geq 0$. Como $y \in \mathbb{Z}$, segue que $y = 0$. Logo, $x^2 = 2$, que gera um absurdo.
Portanto, concluímos assim que 2 é um elemento irredutível em $\mathbb{Z}[u]$ (Para 3 a construção é análoga). ■

Teorema 25. $\mathcal{A}$ *não é um Domínio Euclidiano.*

Demonstração. Suponha por absurdo que $\mathcal{A}$ seja um Domínio Euclidiano. Então existe uma função euclidiana ϕ satisfazendo o algoritmo da divisão Euclidiana. Considere $\phi(n)$ menor possível com $n \neq 0$ e não-unidade. Dividindo 2 por n, temos que existem $q, r \in \mathcal{A}$ tal que

$$2 = nq + r, \ \textit{onde } r = 0 \textit{ ou } \phi(r) < \phi(n).$$

Logo, como $\phi(r)$ e $\phi(n)$ são números naturais, pelo princípio da boa ordem, as únicas possibilidades para $\phi(r)$ são $r = 0$ ou $\phi(r) = \pm 1$. No segundo caso, temos que r é unidade. Portanto, se $r = 0$, então $n|2$. Logo, $n = \pm 2$. Se $r = -1$, então $n|3$, ou seja,

$n = \pm 3$. Além disso, n não pode ser igual a 1 pois assumimos inicialmente que n é não-unidade.
Agora, divida um elemento $\frac{1}{2}\left(1+\sqrt{-19}\right)$ por n. Logo, existem $q', r' \in \mathcal{A}$ tal que

$$\frac{1}{2}\left(1+\sqrt{-19}\right) = nq' + r', \text{ onde } r' = 0 \text{ ou } \phi(r') < \phi(n).$$

Como $\phi(n)$ é suficientemente pequeno, $\phi(r') < \phi(n)$ implica que r' é uma unidade de $\mathcal{A}$ ou $r' = 0$. Note que:

1. Se $r' = -1$, então $u + 1 = nq'$, ou seja, $\frac{u+1}{n} \in \mathcal{A}$. Logo, podemos escrever $\frac{u+1}{n} = x + yu$. Consequentemente,

$$u + 1 = nx + ymu$$

$$(1 - ym)u = nx - 1$$

   Como n e x são inteiros, segue que $(1 - yn) = 0$, ou seja, $yn = 1$. Como n é irredutível, segue que $yn \neq 1$. Portanto, $\frac{u}{n} \in \mathcal{A}$ que gera um absurdo.

2. Se $r' = 0$, então $\frac{1}{n}\left(\frac{1}{2}\left(1+\sqrt{-19}\right)\right) \in \mathbb{A}$, que é uma contradição pela mesma razão do item anterior.

3. Se $r' = 1$, então $\frac{1}{2}\left(1+\sqrt{-19}\right) - 1 = nq$, ou seja, n divide $\frac{1}{2}\left(1+\sqrt{-19}\right) - 1$. Logo, $\frac{1}{n}\left(\frac{1}{2}\left(1+\sqrt{-19}\right) - 1\right) \in \mathcal{A}$, que é uma contradição pela mesma razão do item 1.

■

Portanto, temos que $\mathcal{A}$ não é um Domínio Euclidiano.

Teorema 26. *Mostraremos agora que $\mathcal{A}$ é um Domínio de Ideais Principais.*

Demonstração. Tome $\mathcal{I}$ um ideal não-nulo de $\mathbb{Z}[u]$. Considere $k \in \mathbb{Z}[u]$ não-nulo tal que $|k|$ seja o menor possível. Queremos concluir que existe um elemento k tal que $\mathcal{I} = (k)$. Suponha por absurdo que exista um $\omega \in \mathcal{I}$ tal que $\omega \notin (k)$. Considere $\frac{\omega}{k} \in \mathbb{C}$. Como $u = \frac{1}{2} + \frac{\sqrt{19}}{2}i \in \mathbb{C}$, podemos encontrar um inteiro $z \in \mathbb{Z}$ tal que

$$-\frac{\sqrt{19}}{4} < Im\left(\frac{\omega}{k} + uz\right) < \frac{\sqrt{19}}{4}.$$

Onde Im denota a parte imaginário do número complexo. Dividiremos a demonstração em dois casos.

(Caso 1) Se $-\frac{\sqrt{3}}{2} < Im(\frac{\omega}{k} + uz) \leq \frac{\sqrt{3}}{2}$

Tome um $n \in \mathbb{Z}$ tal que

$$-\frac{1}{2} < Re\left(\frac{\omega}{k} + uz + n\right) \leq \frac{1}{2}$$

onde Re denota a parte real do número complexo. Note que $Im\left(\frac{\omega}{k} + u\omega + n\right) = Im\left(\frac{\omega}{k} + u\omega + n\right)$. Logo,

$$\left|\frac{\omega}{k} + uz + n\right| = \left(Re\left(\frac{\omega}{k} + uz + n\right)\right)^2 + \left(Im\left(\frac{\omega}{k} + uz + n\right)\right)^2 < \left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2$$

Portanto, $|\omega + (uz + n)\, k| = \left|\frac{\omega}{k} + \omega\right||k| < |k|$. Além disso, como $\mathcal{I}$ é ideal, então $(uz + n)\, k \in \mathcal{I}$. Consequentemente, $\omega + (uz + n)\, k \in \mathcal{I}$.

Como tomamos $|k|$ como o menor valor possível e $|\omega + (uz + n)\, k| < |k|$, segue que $\omega + (uz + n)\, k = 0$, ou seja, $\omega \in (k)$, que é um absurdo.

(Caso 2) Ou $-\frac{\sqrt{19}}{4} \leq Im(\frac{\omega}{k} + uz) \leq -\frac{\sqrt{3}}{2}$ ou $\frac{\sqrt{3}}{2} < Im(\frac{\omega}{k} + uz) \leq \frac{\sqrt{19}}{4}$.

Se $-\frac{\sqrt{19}}{4} \leq Im(\frac{\omega}{k} + uz) \leq -\frac{\sqrt{3}}{2}$, escolhemos um elemento $\omega' = -\omega - uzk$.

Se $\frac{\sqrt{3}}{2} < Im(\frac{\omega}{k} + uz) \leq \frac{\sqrt{19}}{4}$, escolhemos um elemento $\omega' = \omega + uzk$.

Como $\mathcal{I}$ é ideal e $\omega, k \in \mathcal{I}$ então $\omega' \in \mathcal{I}$. Além disso, $\omega' \notin (k)$, pois $(k) \not\ni \omega = \pm(\omega' - uzk)$. Portanto, tome $\omega' \in \mathcal{I} - (k)$. tal que $-\frac{\sqrt{3}}{2} \leq Im\left(\frac{\omega'}{k}\right) \leq \frac{\sqrt{3}}{2}$. Portanto, podemos tomar um natural n tal que $-\frac{1}{2}$.

Considere $\omega'' = \omega' + nk \in \mathcal{I}$. Dividindo ambos membros da igualdade por k temos que $\frac{\omega''}{k} = \frac{\omega'}{k} + n$. Como $n \in \mathbb{N}\ (\in \mathbb{R})$, temos que $Im\left(\frac{\omega''}{k}\right) = Im\left(\frac{\omega'}{k}\right)$. Pelo mesmo motivo de ω', o elemento $\omega'' \notin (k)$. Portanto, ω'' é um elemento que não pertence a $\mathcal{I} - (k)$ e

$$\frac{\sqrt{3}}{2} \leq Im\left(\frac{\omega''}{k}\right) \leq \frac{\sqrt{19}}{4}\ e\ -\frac{1}{2} < Re\left(\frac{\omega''}{k}\right) \leq \frac{1}{2}.$$

Note que $u = \frac{1}{2} + \frac{\sqrt{19}}{2}i$ implica em

$$-\frac{3}{2} < Re\left(\frac{2\omega''}{k} - u\right) \leq \frac{1}{2}.$$

Como $\sqrt{19} < 3\sqrt{3}$, temos que

$$\sqrt{3} - \frac{\sqrt{19}}{2} > -\frac{\sqrt{3}}{2}$$

e

$$-\sqrt{3}2 < \sqrt{3} - \frac{\sqrt{19}}{2} \leq Im\left(\frac{2\omega''}{k} - u\right) \leq 0.$$

(Caso 2.1) Se $-\frac{3}{2} < Re\left(\frac{2\omega''}{k} - u\right) \leq \frac{1}{2}$.

De maneira análoga à construção do *Caso 1*, $\left|\frac{2\omega''}{k} - u\right| < \left(\frac{1}{2}\right)^2 + \left(-\frac{\sqrt{3}}{2}\right)^2 = 1$, que implica em $\omega'' = \frac{ku}{2} \in \mathcal{I}$. Note que $u\overline{u} = 5$. Logo, $\frac{5}{2}k = \overline{u}\left(\frac{uk}{2}\right) \in \mathcal{I}$. Como $k \in \mathcal{I}$, temos que $\frac{1}{2}k = \frac{5}{2}k - 2k \in I$. Portanto, se aplicamos o módulo em $\frac{1}{2}k$, temos que $\left|\frac{1}{2}k\right| = \frac{1}{4}|k| < |k|$, que é um absurdo, uma vez que supomos que $|k|$ é o menor valor possível.

(caso 2.2) Se $-\frac{3}{2} < Re\left(\frac{2\omega''}{k} - u\right) \leq -\frac{1}{2}$.

Neste caso, pelo mesmo argumento do *Caso 2.1*,

$$-\frac{1}{2} < Re\left(\frac{2\omega''}{k} - u + 1\right) \leq \frac{1}{2}$$

e

$$-\frac{\sqrt{3}}{2} < Im\left(\frac{2\omega''}{k} - u + 1\right) \leq 0.$$

Logo, $\left|\frac{2\omega''}{k} - u + 1\right| < \left(\frac{1}{2}\right)^2 + \left(-\frac{\sqrt{3}}{2}\right)^2 = 1$. Consequentemente, $|2\omega'' - uk + k| + |k| < |k|$ e $2\omega'' - uk + k = 0$. Portanto, $\frac{u-1}{2}k = \omega'' \in \mathcal{I}$. Agora, basta construir o mesmo argumento do *Caso 2.1* em $(u-1)(\overline{u-1}) = 5$ para encontrar o absurdo, concluindo assim a demonstração.

■

2.3 Números algébricos e transcendentes

Definição 19. Diremos que um elemento n é algébrico se este for raíz de algum polinômio em $\mathbb{Z}[x]$. Caso tal polinômio não exista, diremos que n é transcendente.

Exemplo 12. Todo irracional da forma $\pm\sqrt{d}$, com d livre de quadrados, é um número algébrico, pois é zero do polinômio $x^2 - d$.

Exemplo 13. Todo racional é algébrico. Se $n = \frac{p}{q}$, basta considerar o polinômio $qx - p$ que teremos $q\frac{p}{q} - p = p - p = 0$.

Exemplo 14. O número π é transcendental. Este fato decorre do Teorema de Lindemann–Weierstrass, que nos diz que se e^x é algébrico, então x é transcendente. Como $e^{i\pi} = -1$ é algébrico, então $i\pi$ é transcendente. Como i é algébrico, temos que π é transcedente.

Um resultado interessante sobre os números algébricos é que o conjunto $\mathbb{R}$ formado por todos estes números é contável, ou seja, podemos exibir uma função que leva elementos deste conjunto nos naturais. Tal fato foi demonstrado pelo matemático alemão Georg Cantor. Disso temos que o conjunto $\mathcal{B}$ dos números transcendentais é incontável, visto que $\mathbb{R}$ é incontável, $\mathbb{R} = \mathcal{A} \cup \mathcal{B}$ e união de conjuntos contáveis é contável.
A partir deste resultado, temos um fato interessante. A densidade dos Números Reais não vem do conjunto dos Números Irracionais propriamente falando, mas do conjunto dos Números Transcendentes.
Tudo que foi escrito sobre os números algébricos, propicia ferramentas par construir estes números. Disso surge uma indagação: É possível explicítar uma construção dos números transcendentes? O teorema de Liouville, que será enunciado a seguir, apresenta um argumento que diz que a resposta é sim.

Teorema 27. *Considere a um número algébrico onde a é raíz de um polinômio irredutível f sobre $\mathbb{Z}$ com $\delta(f) = n > 1$. Portanto, existe uma constante k tal que para todo número racional $\frac{m}{n}$, temos que*

$$\left| a - \frac{p}{q} \right| > \frac{k}{q^n}$$

.

Demonstração. Suponha que $\left|\alpha - \frac{p}{q}\right| > 1$. Para que a desigualdade seja verdade, basta tomar $k = 1$.
Agora, suponha que $\left|\alpha - \frac{p}{q}\right| \geq 1$. Pelo teorema do Valor Médio em f no intervalo $(\alpha, \frac{p}{q})$, temos que:

$$\frac{f(\alpha) - f\left(\frac{p}{q}\right)}{\alpha - \frac{p}{q}} = f'(\beta).$$

Desde que α é raíz de f, temos que $f(\alpha) = 0$. Além disso, como f é irredutível sobre $\mathbb{Z}$, então f não possuí uma raíz racional.
Note que $q^n f\left(\frac{p}{q}\right)$ é um número inteiro, pois se escrevermos $f(x) = a_0 + a_1 x + \ldots + a_n x^n$,

[0] A equação decorre da identidade de Euler dada por $e^{i\pi} = -1$

então temos que:

$$q^n f\left(\frac{p}{q}\right) = q^n\left(a_0 + a_1\frac{p}{q} + \ldots + a_n\frac{p^n}{q^n}\right) = a_0q^n + a_1pq^{n-1} + \ldots + a_np^n$$

.

Portanto,

$$\left|f\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}.$$

Como $\beta \in (\alpha, \frac{p}{q})$ e $\left|\alpha - \frac{p}{q}\right| \leq 1$, então $|\beta - \alpha| < 1$. Logo, pela continuidade de f', temos que $|f'(\beta)| < \frac{1}{x_0}$ para todo número entre 1 e β. Concluí-se que

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f\left(\frac{p}{q}\right)}{f'(\beta)}\right| > \frac{1}{q^n}x_0$$

■

Lema 28. *O número* $\zeta = \sum_{n=1}^{\infty} 10^{-k!}$ *é transcendente.*

Demonstração. Seja $\frac{p_r}{q_r} = \sum_{k=1}^{r} 10^{-k!}$. Note que, em cada $\frac{p_i}{q_i}$, o denominador q_i é igual à $10^{i!}$. Portanto,

$$\left|\zeta - \frac{p_r}{q_r}\right| = \left|\sum_{n=1}^{\infty} 10^{-n!} - \sum_{k=1}^{r} 10^{-k!}\right| = \left|\sum_{n=r+1}^{\infty} 10^{-n!}\right| = \sum_{n=r+1}^{\infty} 10^{-n!} < \frac{2}{10^{(r+1)!}} = \frac{2}{{q_r}^{r+1}}$$

Agora, suponha que ζ é um número algébrico, então existe um polinômio p de menor grau n tal que $p(\zeta) = 0$. Pelo teorema anterior, existe uma constante k tal que $\left|\zeta - \frac{p}{q}\right| > \frac{k}{q^n}$ para todo número $\frac{p}{q}$. Fazendo $\frac{p}{q} = \frac{p_r}{q_r}$, temos que

$$\left|\zeta - \frac{p_r}{q_r}\right| = \sum_{n=r+1}^{\infty} 10^{-n!} > \frac{k}{{q_r}^{r+1}}$$

Que é uma contradição. ■

2.4 Polinômio minimal

Nesta seção, iremos definir a ideia de polinômio minimal e analisar algumas propriedades necessárias para o andamento do trabalho.

Definição 20. Diremos que p é o polinômio minimal de t, se p é o polinômio mônico de menor grau que satisfaz $p(t) = 0$.

Em geral, utilizaremos $m(t)$ para denotar o polinômio minimal de t sobre $\mathbb{Q}$

Lema 29. *Se m é o polinômio minimal de um elemento algébrico α, então m é irredutível.*

Demonstração. Suponha por absurdo que $m(t) = f(t)g(t)$. Sabemos que $f(\alpha) = 0$, logo, $f(\alpha)g(\alpha) = 0$. Como estamos trabalhando, a priori, sobre $\mathbb{R}$ e este é um domínio, então $f(\alpha)g(\alpha) = 0$ implica que $f(\alpha) = 0$ ou $g(\alpha) = 0$. Contudo, $\delta(f) < \delta(m)$, o que contradiz o fato de m ser o polinômio minimal. ■

Na demonstração não foi explicitado mas os casos triviais $f(t) = 1$ e $g(t) = m(t)$ ou $g(t) = 1$ e $f(t) = m(t)$ não necessitam de demonstração por motivos óbvios.

Corolário 30. *O conjunto formado por todos os números algébricos $\mathcal{A}$ formam um corpo.*

Demonstração. Suponha que

$$p(x) = \sum_{i=0}^{n} a_i x^i.$$

Como x é diferente de zero, então podemos reescrever o termo geral do somatório como $a_i x^i \frac{x^n}{x^n}$. Portanto,

$$p(x) = x^n \sum_{i=0}^{n} a_i \frac{x^i}{x^n} = x^n \left(\frac{a_0}{x^n} + \frac{a_1}{x} x_n + \ldots + \frac{a_n x^n}{x^n} \right) = x^n \left(\frac{a_0}{x^n} + \frac{a_1}{x^n} x + \ldots + \frac{a_n}{x^n} x^n \right)$$

$$= x^n \left(a_0 x^{-n} + a_1 x^{1-n} + \ldots + a_n \right).$$

Disso, temos que $(a_0 a^{-n} + a_1 a^{1-n} + \ldots + a_n) = 0$
Considere o polinômio q dado por

$$q(x) = \sum_{j=0}^{n} \frac{a_j}{\left(x^{-1}\right)^n} x^j = \sum_{j=0}^{n} a_j x^{n-j}$$

. Avaliando o polinômio em $x = a^{-1}$, temos que

$$q(a^{-1}) = \sum_{j=0}^{n} a_j \left(a^{-1}\right)^{n-j} = \sum_{j=0}^{n} a_j a^{j-n} = \left(a_0 a^{-n} + a_1 a^{1-n} + \ldots + a_n \right) = 0.$$

Portanto, segue que a^{-1} é algébrico. ■

Corolário 31. *Se a e b são números algébricos, então $a+b$, $a-b$ e ab são algébricos.*

Para verificar esses resultados, é necessário uma proposição que iremos demonstrar mais a frente.

Lema 32. *Considere o elemento a sendo a raiz de $f(x) \in \mathbb{Q}[x]$. Se $m(x)$ polinômio minimal, então este dividirá f(x).*

Demonstração. Pelo algoritmo da divisão euclidiana em $\mathbb{Q}[x]$, existem polinômios q e r tal que:

$$f(x) = m(x)q(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } \delta(r(x)) < \delta(m(x))$$

Se $r(x) = 0$, nada a fazer. Suponha que $\delta(r(x)) < \delta(m(x))$. Então, substituindo a equação por $x = a$, teremos que

$$f(a) = m(a)q(a) + r(a) \implies 0 = 0 + r(a)$$

Portanto, a é raíz de r e r tem menor grausque m. Isto gera um absurdo, uma vez que supomos que m é o polinômio minimal de a.

■

Para deixar mais claro o conceito de polinômio minímo, usaremos o exercício abaixo.

Exemplo 15. Encontre o polinômio minimal de $a = \sqrt{3} + \sqrt{5}$ sobre $\mathbb{Q}$.

Solução. Tomando $u = \sqrt{3} + \sqrt{5}$, então

$$u^2 = \left(\sqrt{3} + \sqrt{5}\right) = 8 + 2\sqrt{15} \implies u^2 - 8 = \sqrt{15}$$

Como a equação acima possui coeficientes não-racionais, então $x^2 - 8 - \sqrt{15} \notin \mathbb{Q}[x]$. Portanto, $(x^2-8)^2 = x^4 - 18x^2 + 64 = 15$ é o polinômio mínimo de $\sqrt{3} + \sqrt{5}$.

Teorema 33. *Se a é um elemento algébrico, então a extensão $\mathbb{Q}(a)$ é igual é igual ao conjunto dos polinômios $\mathbb{Q}[a]$, ou seja, cada elemento da extensão pode ser escrito como um polinômio de a.*

Demonstração. Basicamente, o conjunto $\mathbb{Q}(a)$ contém os elementos gerados pelas operações aritméticas dos números racionais com o elemento algébrico a. Portanto, o conjunto

em questão corresponde aos quociente de polinômios $\frac{p(a)}{q(a)}$. Portanto, para concluir que $\mathbb{Q}(a) = \mathbb{Q}[a]$, é suficiente mostrar que o quociente $\frac{p(a)}{q(a)}$ ainda é um polinômio em a.
Seja $m(x)$ o polínomio minimal de a sobre $\mathbb{Q}$. Por definição, o mdc de $m(x)$ e $q(x)$ é no máximo $m(x)$. Como $m(x)$ é minimal, então $m(x)$ é irredutível. Portanto, $mdc\,(m(x), q(x)) = 1$ ou $mdc\,(m(x), q(x)) = m(x)$. Note que a única possibilidade real é $mdc\,(m(x), q(x)) = 1$, pois $mdc\,(m(x), q(x)) = m(x)$ implicaria em $q(a) = 0$, mas claramente $q(a) \neq 0$.
Agora, usaremos o algoritmo da Divisão Euclidiana para explicitar o polinômio associado à $\frac{p(a)}{q(a)}$.
Pela identidade de Bézout, existem $r(x)$ e $s(x)$ tais que para qualquer que seja o $x \in \mathbb{Q}$,

$$r(x)q(x) + s(x)m(x) = mdc\,(m(x), q(x)) = 1.$$

Em particular, $r(a)q(a) + s(a)m(a) = 1$. Como $m(x)$ é minimal de a, $m(a) = 0$. Portanto, $r(a)q(a) = 1$. Multiplicando ambos os lados por $\frac{p(a)}{q(a)}$, temos que $r(a)p(a) = \frac{p(a)}{q(a)}$, concluindo assim a demonstração. ■

Além das caracterizações mostradas anteriormente, um resultado decorrente dsse teorema nos dá mais ferramentas para verificar se um número é algébrico.

Corolário 34. *Seja a um número complexo. As sentenças abaixo são equivalentes:*

a) a é um elemento algébrico;

b) a extensão de corpos $\mathbb{Q}(a)/\mathbb{Q}$ tem grau finito.

Demonstração. $(a) \implies (b)$. Suponha que a é um elemento algébrico. Denote por $m(x) = a_n x^n + ... + a_1 x + a_0$ o polinômio minimal de a. Ou seja,

$$a_n a^n + ... + a_1 a + a_0 = 0$$

Dividindo ambos os lados por a_n, temos que

$$a^n + ... + \frac{a_1}{a_n} a + \frac{a_0}{a_n} = 0$$

$$a^n = -\left(\frac{a_{n-1}}{a_n} a^{n-1} + ... + \frac{a_1}{a_n} a + \frac{a_0}{a_n}\right) \tag{2.3}$$

Seja q um elemento em $\mathbb{Q}(a)$. Como a é algébrico, então q pode ser escrito como um

polinômio aplicado em a. Se o grau desse polinômio é maior que n, então pela equação 2.3, podemos reduzir o polinômio a:

$$c_{n-1}a^{n-1} + \ldots + c_1 a + c_0.$$

Verificaremos se esse polinômio é único. Suponha que exista outro polinômio tal que $a^n = b_{n-1}a^{n-1} + \ldots + b_1 a^1 + b_0$.
Portanto,

$$(c_{n-1} - b_{n-1})\, a^{n-1} + ... + (c_1 - b_1)\, a + (c_0 - b_0) = 0,$$

que gera um absurdo, afinal supomos que o polinômio minimal de a tem grau n. Logo, cada elemento é gerado de maneira única por $1, a, \ldots, a^{n-1}$.
Se olharmos $\mathbb{Q}(a)$ como um espaço vetorial sobre $\mathbb{Q}$, então $\dim_{\mathbb{Q}} \mathbb{Q}(a) = n$. Conclui-se que $[\mathbb{Q}(a) : \mathbb{Q}]$ é finito.
$b) \implies a)$. Suponha que $[\mathbb{Q}(a) : \mathbb{Q}] = n$. Então, quaisquer $n+1$ vetores de $\mathbb{Q}(a)$ sobre $\mathbb{Q}$ são linearmentes dependentes. Em particular, $1, \ldots, a^{n-1}$, são LDs. Portanto,

$$a_n a^n + ... + a_1 a + a_0 = 0$$

■

Demonstração do corolário 23. Primeiro, verificamos se a soma de elementos algébricos é algébrico.
Pela proposição anterior, $[\mathbb{Q}(a) : \mathbb{Q}]$ e $[\mathbb{Q}(b) : \mathbb{Q}]$ são finitos. Suponha que $[\mathbb{Q}(a) : \mathbb{Q}] = n$ e $[\mathbb{Q}(b) : \mathbb{Q}] = m$. Sabemos que $[\mathbb{Q}(a, b) : \mathbb{Q}]$ é finito. Portanto, basta concluir que $\mathbb{Q}(a + b) \subseteq \mathbb{Q}(a, b)$ que teremos que $a + b$ é algébrico.
Note que os elementos de $\mathbb{Q}(a, b)$ são da forma $\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} c_{ij} a^i b^j$. Basta analisar que

$$a + b = 1.a^1 b^0 + \ldots + 0a^{m-1} b^0 + \ldots + 1.a^0 b^1 + \ldots + 0a^{m-1} b^{n-1}.$$

Logo, $\mathbb{Q}(a + b) \subseteq \mathbb{Q}(a, b)$. Consequentemente, $[\mathbb{Q}(a + b) : \mathbb{Q}] \leq [\mathbb{Q}(a, b) : \mathbb{Q}]$.
O argumento de $a - b$, ab e $\frac{a}{b}$ é análoga. Basta escolher as constantes convenientes. ■

2.5 Corpos numéricos

A partir da motivação da enumerabilidade de $\mathcal{A}$ é algébrico, iremos exibir alguns resultados interessantes sobre *corpos numéricos* a partir das extensões de corpos e da algebricidade dessos elementos dessas estruturas.
Como não haviamos feito antes, é necessário inicialmente definir o que seriam essas novas estruturas.

Definição 21. Um corpo $\mathbb{K}$ é dito um *corpo numérico* se $[\mathbb{K} : \mathbb{Q}] < \infty$.

Definição 22. O grau de $\mathbb{K}$ é o grau da extensão de corpos $[\mathbb{K} : \mathbb{Q}]$, ou seja, a dimensão de $\mathbb{K}$ como um $\mathbb{Q}$-espaço vetorial.

Exemplo 16. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ é um corpo numérico de grau finito, pois todo elemento é combinação linear dos elementos 1 e $\sqrt{2}$, então $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Exemplo 17. $\mathbb{Q}(\pi)$ não é um corpo número, afinal π é trascendente e portanto não satisfaz nenhuma equação polinomial sobre $\mathbb{Q}$. Logo, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ é infinito.

Uma observação importante é que todo corpo numérico contém $\mathbb{Q}$ (afinal, $\mathbb{Q}$ é o menor corpo numérico) e em decorrência disso possui característica 0.
Um resultado interessante é que toda extensão é gerada por um único elemento. Para verificar esse fato é necessário um lema preliminar. A demonstração do lema requer apenas algoritmo da divisão euclidiana e outros resultados que já apresentamos. Por conta de seu tamanho, iremos apenas enuncia-lo.

Lema 35. *Seja $p(x) \in \mathbb{Q}[x]$ um polinômio irredutível. Então, o polinômio possui raízes distintas em $\mathbb{C}$.*

O resultado é mais geral. Em qualquer que seja o corpo de característica 0, um polinômio irredutível tem raízes distintas. Entretanto, para o que vamos construir, é necessário apenas o que foi enunciado.

Teorema 36 (Elemento primitivo)**.** *Suponha que $\mathbb{K} \subseteq \mathbb{L}$ seja uma extensão de corpos com característica zero. Então, $\mathbb{L} = \mathbb{K}(c)$ para certo $c \in \mathbb{L}$.*

Demonstração. Suponha que $\mathbb{L}$ seja gerado sobre $\mathbb{K}$ por n elementos. Inicialmente, mostraremos o caso onde $n = 2$ e depois generalizaremos.

Suponha que $\mathbb{L} = \mathbb{K}(a, b)$, onde a e b são elementos algébricos. Considere que p e q sejam seus polinômios minimais, respectivamente. Por $\mathbb{C}$ ser algebricamente fechado, se $\delta(p) = s$ e $\delta(q) = t$, então p e q tem exatamente s e t raízes, contanto com a multiplicidade. Denotemos as raízes de p por $\alpha_1, \ldots, \alpha_s$ e as raízes de q por $\beta_1, \ldots, \beta_t$.
Pelo lema anterior, p e q possuem raízes distintas em $\mathbb{C}$. Portanto, a única solução do polinômio

$$a_i + xb_j = a_1 + xb_1$$

é o elemento $x = \frac{a_j - a_1}{b_1 - b_j}$ (Note que para cada i,j teremos um x, a priori, diferente). Tome k um elemento diferente de x. Como k não é solução de nenhuma das equações, segue que $a + cb \neq a_i + cb_j$. Assuma que $c = a + kb$ gera $\mathbb{L}$ sobre $\mathbb{K}$. Claramente $c \in \mathbb{K}(a, b)$, pois, como mostramos anteriormente, basta escrever $c = a + kb = 1ab^0 + ka^0b$. Portanto, para concluir a demonstração para o caso $n = 2$, é suficiente mostrar que $a, b \in \mathbb{K}(c)$.
Note que, os polinômios $q(x)$ e $p(c - kx)$ possuem coeficientes em $\mathbb{K}(c)$ e b como raíz. Além disso, as demais raízes de $q(x)$ são $b_2, ..., b_n$. Note que $c - kb_j$ é diferente de a para todo j. Portanto, $mdc(q(x), p(c - kx)) = (x - b)$. Claramente o mdc de dois polinômios contém os coeficientes de ambos. Logo, $(x - b)$ tem coeficientes em $\mathbb{K}(c)$, isto é, $b \in \mathbb{K}(c)$. Por fim, $a = c - kb \in \mathbb{K}(c)$.
Iremos agora utilizar o fato acima para generalizar o caso quando $m > 2$. Note que, se $L = \mathbb{K}(a_1, a_2, \ldots, a_m)$, então $L = \mathbb{K}(a_1, a_2, \ldots, a_{m-2})(a_{m-1}, a_m)$. Pelo caso anterior, existe um c_{m-1} tal que $\mathbb{K}(a_1, a_2, \ldots, a_{m-2})(a_{m-1}, a_m) = \mathbb{K}(a_1, a_2, \ldots, a_{m-2})(c_{m-1})$. Basta repetir o processo até que reste apenas um elemento e então o resultado segue. ■

Corolário 37. *Seja $\mathbb{K}$ um corpo numérico. Então $\mathbb{K} = \mathbb{Q}(c)$ para certo c.*

Demonstração. O resultado é uma aplicação direta do Teorema 36. ■

Para melhor compreensão, iremos mostrar alguns exemplos práticos do teorema em corpos numéricos (que é nosso foco).

Exemplo 18. Pelo teorema do elemento primitivo, mais especificamente pelo corolário, existe um elemento c tal que o corpo numérico $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ é igual a $\mathbb{Q}(c)$. Usando a mesma construção do teorema, é possível tomar um k tal que $c = \sqrt{3} + k\sqrt{5}$. Tome $k = 1$. Logo, $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Elevando ambos os membros da igualdade de c ao cubo, teremos que:

$$c^3 = \left(\sqrt{3} + \sqrt{5}\right)^3$$

$$c^3 = \left(8 + 2\sqrt{15}\right)\left(\sqrt{3} + \sqrt{5}\right)$$

$$c^3 = 8\sqrt{3} + 8\sqrt{5} + 3\sqrt{5} + 5\sqrt{3}$$

$$c^3 = 13\sqrt{3} + 11\sqrt{5}.$$

Portanto, podemos escrever ambas as raízes como polinômios em c, onde

$$c^3 = 11c + 2\sqrt{3}$$

$$\frac{c^3 - 11c}{2} = \sqrt{3}$$

e

$$\frac{13c - c^3}{2} = \sqrt{5}$$

Portanto, $\sqrt{3}, \sqrt{5} \in \mathbb{Q}(c)$. Logo, $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \subseteq \mathbb{Q}(c)$. Além disso,

$$\sqrt{3} + \sqrt{5} = 1.\sqrt{3}\left(\sqrt{5}\right)^0 + 1.\left(\sqrt{3}\right)^0\sqrt{5}.$$

Concluimos a outra inclusão e, portanto, $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(c)$.

2.6 Integralidade

A partir de agora, iremos fazer um estudo das extensões de $\mathbb{Q}$ assim como fazemos para os inteiros. Iremos utilizar as definições gerais de irredutibilidade, primalidade e divisibilidade de elementos e polinômios. Por exemplo, quando for dito que um elemento n não-inversível é primo, queremos dizer que se $n|ab$ então $n|a$ ou $n|b$. Além disso, usaremos a notação $\mathcal{O}_{\mathbb{K}}$ para denotar o conjunto dos inteiros sobre $\mathbb{K}$.

Definição 23. Seja a um elemento algébrico. Diremos a é um inteiro algébrico quando seu polinômio mônico possui coeficientes inteiros.

Exemplo 19. Todo número inteiro k é um inteiro algébrico, pois $x - k$ tem coeficientes em $\mathbb{Z}$.

Exemplo 20. Os elementos da forma $\sqrt{d}$, onde $d \in \mathbb{Z}$ são inteiros algébricos, pois são raízes do polinômio da forma $m(x) = x^2 - d$ e este, por sua vez, possui coeficientes inteiros.

Exemplo 21. Claramentes os elementos trascendentes não são inteiros algébricos.

Exemplo 22. O elemento $\frac{1-\sqrt{7}}{2}$ não é um inteiro algébrico, pois seu polinômio mônico associado é $x^2 - x - \frac{3}{2}$, pois o termo livre não pertence a $\mathbb{Z}$. Em contrapartida, o elemento $\frac{1-\sqrt{-7}}{2}$ é um inteiro algébrico pois seu polinômio mônico associado é $x^2 - x + 2$.

Lema 38. *Se a satisfaz qualquer polinômio mônico com coeficientes inteiros, então a é um inteiro algébrico.*

Demonstração. Suponha que p seja um polinômio mônico em $\mathbb{Z}[x]$. Além disso, assuma que $p(a) = 0$. Seja $m(x) \in \mathbb{Q}[x]$ o polinômio minimal de a sobre $\mathbb{Q}$. Iremos mostrar que o minimal também tem coeficientes em $\mathbb{Z}$.
Sabemos que o polinômio minimal divide o polinômio p. Então, $p(x) = m(x)q(x)$, onde q é um certo polinômio de $\mathbb{Q}[x]$. Note que $q(x)$ mônico, afinal, $p(x)$ e $m(x)$ são mônicos.
Tome α e β elementos inteiros tal que $\alpha q(x)$ e $\beta m(x)$ sejam polinômios com coeficientes inteiros de modo que mdc entre os coeficientes seja igual a 1. (α e β podem ser tomados como o *mmc* dos denominadores de ambos polinômios, por exemplo). Portanto,

$$(ab)f(x) = aq(x)bm(x)$$

Suponha que $ab \neq 1$. Tome p primo tal que $p|ab$. Então $p|(ab)f(x)$. Isso implica em $p|a$ ou $p|b$. Consequentemente, existem coeficientes em $aq(x)$ e em $bm(x)$ que não são divisíveis por p. Logo, o produto desses coeficientes não é divisível por p. Por outro lado, o polinômio $(ab)f(x)$ tem todos os coeficientes divisível por ab, em particular, por p. Conclui-se que $ab = 1$. Como a e b são inteiros, segue que $a = b = 1$. Essa afirmação gera uma contradição, já que supomos que $ab \neq 1$.
Portanto, $m(x)$ e $q(x)$ tem coeficientes sobre $\mathbb{Z}$. ■

A demonstração do teorema acima basicamente implica no Lema de Gauss para polinômios, que diz *se um polinômio com coeficientes inteiros é irredutível sobre $\mathbb{Z}$, então o polinômio também é irredutível sobre $\mathbb{Q}$.*

Exemplo 23. O número $\frac{1+\sqrt{5}}{2}$ é um inteiro algébrico. Tomando $u = \frac{1+\sqrt{5}}{2}$, temos que

$$4u^2 = 1 + 2\sqrt{5} + 5$$

$$4u^2 - 4 = 2 + 2\sqrt{5}$$

$$u^2 - 1 = \frac{1+\sqrt{5}}{2}$$

$$u^2 - u - 1 = 0$$

Logo, $\frac{1+\sqrt{5}}{2}$ é raíz do polinômio $p(x) = x^2 - x - 1$. Como $p(x)$ é mônico e possui apenas coeficientes inteiros, segue pelo *Lema 30* que $\frac{1+\sqrt{5}}{2}$ é um inteiro algébrico.

Exemplo 24. O número $v = \frac{1+\sqrt{3}}{\sqrt{2}}$ é um inteiro algébrico. Pois

$$2v^2 = 1 + 2\sqrt{3} + 3$$

$$2v^2 - 4 = 2\sqrt{3}$$

$$4v^4 - 16v^2 + 16 = 12$$

$$4v^4 - 16b^2 + 4 = 0$$

$$v^4 - 4v^2 + 1 = 0$$

Pelo mesmo argumento do exemplo anterior, segue que $\frac{1+\sqrt{3}}{\sqrt{2}}$ é um inteiro algébrico.

2.7 Anel dos inteiros algébricos

Anteriormente, verificamos que o conjunto dos números algébricos $\mathcal{A}$ formam um corpo (em particular, um anel). Nesta sessão, estamos interessados em verificar se a restrição do conjunto para apenas os inteiros algébricos $\mathcal{I}$ formam, ao menos, um anel.
Nesta perspectiva, será necessário introduzir alguns nomenclatura sobre *módulos*. Vale salientar que nosso foco não é analisar a teoria de módulos e passaremos apenas na sua *borda* utilizando alguns conceitos, entretanto, para ficar claro com o que estamos trabalhando, iremos definir o que é essa estrutura algébrica.

Definição 24. Seja $\mathcal{R}$ um anel. Um grupo abeliano $\mathcal{M}$ é chamado $\mathcal{R} - modulo$ se existe um mapa

$$\phi : \mathcal{R} \times \mathcal{M} \longrightarrow \mathcal{M}$$

$$(r, m) \longmapsto rm$$

tal que

a) $r(m_1 + m_2) = rm_1 + rm_2$

b) $(r_1 + r_2)m = r_1m + r_2m$

c) $r_1(r_2m) = (r_1r_2)m$

para quaisquer que sejam os $r, r_1, r_2 \in \mathcal{R}$ e $m, m_1, m_2 \in \mathcal{M}$. Se $\mathcal{R}$ é um anel com unidade, então o mapa deve satisfazer também a propriedade de que para todo $m \in \mathcal{M}$, $1_{\mathcal{R}}m = m$. Podemos fazer uma analogia com a definição de módulo e a de espaço vetorial. Em álgebra linear trabalhamos com espaços vetoriais sobre um dado corpo $\mathbb{K}$. Enfraquecermos a necessidade de $\mathbb{K}$ ser corpo e trabalhamos com módulos sobre um dado anel $\mathcal{R}$.

Exemplo 25. $\mathbb{Z}[\alpha]$ é um módulo sobre $\mathbb{Z}$, pois $\mathbb{Z}[\alpha]$ é anel e $\mathbb{Z} \subset \mathbb{Z}[\alpha]$, logo as propriedades de módulo são válidas.

Definição 25. Diremos que um módulo $\mathcal{M}$ é *finitamente gerado* sobre $\mathcal{R}$ quando existem um número finito de elementos $r_1, \ldots, r_n$ tal que para todo $m \in \mathcal{M}$, existem $a_1, \ldots, a_n \in \mathcal{R}$

$$a_1r_1, \ldots, a_nr_n = m.$$

Também pode-se notar nesta definição uma semelhança com a álgebra linear, quando falamos de espaços vetoriais de dimensão finita.

Proposição 39. *Seja $\alpha \in \mathbb{C}$. Então, os itens abaixo são equivalentes:*

a) α é um inteiro algébrico.

b) $\mathbb{Z}[\alpha]$ é finitamente gerado sobre $\mathbb{Z}$.

Demonstração (a) $\Longrightarrow$ (b). Suponha que α é um inteiro algébrico. Então, α é raiz de algum polinômio mônico $p(x) \in \mathbb{Z}[x]$ onde $\delta(p) = n_0$ para certo $n_0 \in \mathbb{N}$. Tome um polinômio qualquer $g(x)$ em $\mathbb{Z}[x]$. Pela divisão euclidiana, temos que

$$g(x) = q(x)p(x) + r(x).$$

para certos $r(x), q(x) \in \mathbb{Z}[x]$, com $r(x) = 0$ ou $\delta(x) < n_0$. Tome $x = \alpha$. Logo,

$$g(\alpha) = q(\alpha)p(\alpha) + r(\alpha)$$

$$g(\alpha) = q(\alpha)0 + r(\alpha)$$

$$g(\alpha) = r(\alpha).$$

Logo, todo polinômio $g(\alpha)$ tem grau menor que n_0 e pode ser escrito como uma combinação de linear de $1+\alpha+\ldots+\alpha^{n_0-1}$, com coeficientes em $\mathbb{Z}$. Ou seja, $\mathbb{Z}[\alpha]$ é finitamente gerado em $\mathbb{Z}$.

(b) $\implies$ *(a)* Suponha que $Z[\alpha]$ é finitamente gerado sobre $\mathbb{Z}$ por $m_1, \ldots, m_{n_0}$. Como $\alpha m_i \in \mathbb{Z}[\alpha]$, então

$$\alpha m_i = \sum_{j=1}^{n} a_{ij} m_i$$

onde $a_{ij} \in \mathbb{Z}$. Construa a matriz $A = (a_{ij})$. Logo, se $\mathbf{v} = m_i$, então $A\mathbf{v} = \alpha\mathbf{v}$. Do modo como construimos, temos que α é um autovalor de A e $\mathbf{v}$ um autovetor. Ou seja, α é raíz do polinômio característico, que é mônico. Como cada entrada de A pertence a $\mathbb{Z}$, o resultado segue. ■

Corolário 40. *Seja $\mathcal{R} \subset \mathbb{Z}$ um anel. Se $\mathcal{R}$ é finitamente gerado sobre $\mathbb{Z}$, então todo elemento $a \in \mathcal{R}$ é raíz de um polinômio mônico com coeficientes inteiros.*

Proposição 41. *Suponha que a e b sejam inteiros algébricos. Logo, $\mathbb{Z}[a, b]$ é finitamente gerado como um $\mathbb{Z} - modulo$.*

O próximo corolário nos dá o objetivo dessa sessão.

Corolário 42. *O conjunto de todos os inteiros algébricos formam um anel. Sejam a e b inteiros algébricos. Note que $a + b \in \mathbb{Z}$ pois $a + b = 1.a^1.b^0 + 1.a^0.b^1$. Logo, pela proposição anterior, temos que $\mathbb{Z}[a, b]$ é finitamente gerado como $\mathbb{Z}$-módulo. Além disso, a Proposição 34 implica que $a + b$ é um inteiro algébrico.*
Para $a - b$ e ab, o argumento é análogo pois $a - b = 1.a^1.b^0 + (-1).a^0b^1$ e $ab = 1a^1b^1$.

2.8 Os inteiros algébricos em corpos numéricos

Nas seções anteriores, já comentamos que todo corpo numéricos contém $\mathbb{Q}$ (pois $\mathcal{Q}$ é o menor corpo numéricos. Falaremos agora dos inteiros em corpos numéricos.

Definição 26. Seja $\mathbb{K}$ um corpo numérico. O conjuntos dos inteiros em $\mathbb{K}$ é denotado por

$$\mathcal{O}_{\mathbb{K}} = \{a \in \mathbb{K} \mid a \text{ é um inteiro algébrico}\}.$$

Mostraremos agora alguns resultados sobre os o anel dos inteiros algébricos de um corpo numérico e alguns exercícios.

Corolário 43. *Se $\mathbb{K}$ é um corpo numérico, então $\mathcal{O}_{\mathbb{K}}$ é um anel.*

Demonstração. Tome $a, b \in \mathcal{O}_{\mathbb{K}}$. Como $\mathbb{K}$ é um corpo, então $a+b$, $a-b$ e ab pertencem à $\mathbb{K}$. Além disso, já mostramos anteriormente que a soma, diferença e produto de inteiros algébricos ainda é um inteiro algébrico. Logo, $a+b$, $a-b$ e ab pertencem à $\mathcal{O}_{\mathbb{K}}$. ■

Corolário 44. *Suponha que $\mathcal{R}$ seja um anel de um corpo numérico $\mathbb{K}$ e $\mathcal{R}$ seja finitamente gerado como um $\mathbb{Z}-$módulo, então $\mathcal{R} \subseteq \mathcal{O}_{\mathbb{K}}$.*

Demonstração. Já mostramos que se $\mathcal{R}$ é um anel contendo $\mathbb{Z}$ e $\mathcal{R}$ é finitamente gerado, então todo elemento a de $\mathcal{R}$ é raíz de um polinômio mônico com coeficientes em $\mathbb{Z}$. Logo, a é um inteiro algébrico para todo $a \in \mathcal{R}$. Conclui-se que $\mathcal{R} \subseteq \mathcal{O}_{\mathbb{K}}$. ■

Proposição 45. *Suponha que d seja um inteiro livre de quadrados, então*

1. *Se $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$, então o anel dos inteiros em $\mathbb{Q}\left(\sqrt{d}\right)$ é dada por*
$$\mathbb{Z}\left[\sqrt{d}\right] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}.$$
2. *Se $d \equiv 1 \pmod 4$, então o anel dos inteiros em $\mathbb{Q}\left(\sqrt{d}\right)$ é dada por*
$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) \;\middle|\; a, b \in \mathbb{Z}\right\}.$$

Demonstração. Seja $\alpha = x + y\sqrt{d}$ com $x, y \in \mathbb{Q}$. Logo,

$$(\alpha - x)^2 = y^2 d$$

$$\alpha^2 - 2x\alpha + x^2 - y^2 d = 0.$$

Note que, para que as condições para que o polinômio mônico acima ser inteiro é de que

$$2x \in \mathbb{Z}$$

$$x^2 - y^2 d \in \mathbb{Z}.$$

Pela primeira condição, temos que a é um número inteiro ou $a = \frac{k}{2}$ onde k é ímpar. Se a é inteiro, então b^2d é inteiro e como d é livre de quadrados, segue que b é inteiro. Além disso, $\mathbb{Z}[\sqrt{d}]$ sempre contém $\mathbb{Z}$ pois $\mathbb{Z} = \mathbb{Z} + 0\mathbb{Z}$.
Se $a = \frac{k}{2}$, então

$$\frac{k^2}{2^2} - y^2d \in \mathbb{Z},$$

ou

$$4| \left(k^2 - 4y^2d\right).$$

Logo, $4y^2d \in \mathbb{Z}$. Como d é livre de quadrados, segue que $2y$ é inteiro. Ou seja, y não é um inteiro. Portanto,

$$\frac{k^2}{2^2} - y^2d \notin \mathbb{Z}.$$

Consequentemente, $4y^2$ é um inteiro ímpar. Logo,

$$k^2 - 4y^2d \equiv 0 \pmod 4.$$

Além disso, sabemos que se k é ímpar, então $k^2 \equiv 1 \pmod 4$, o mesmo para $4y^2$. Então,

$$1 - d \equiv 0 \pmod 4.$$

Note que se $d \equiv 1 \pmod 4$, então

$$\mathcal{O}_{\mathbb{Q}[\sqrt{d}]} = \left\{ x + y\sqrt{d} \mid Ou\ x, y \in \mathbb{Z},\ ou\ x = \frac{k}{2}\ e\ y = \frac{q}{2},\ onde\ k, q\ são\ inteiros\ ímpares \right\}$$

Note que, se $x = \frac{k}{2}$ e $y = \frac{q}{2}$, então

$$\frac{k-q}{2} + \frac{q}{2} + \frac{q}{2}\sqrt{d} = \frac{k-q}{2} + q\left(\frac{1+\sqrt{d}}{2}\right).$$

Independente de quem sejam k e q, temos que $k - q$ é par, logo $\frac{k-q}{2}$ é inteiro. Juntando com o caso onde x, y são inteiros, o resultado *2* segue. Se $d \not\equiv 1 \pmod 4$, então o o resultado *1* segue. ■

Capítulo 3

Fatoração Única em Ideais

Neste capítulo iremos desenvolver o objetivo principal deste trabalho. Verificaremos que o anel $\mathbb{Z}[\sqrt{-5}]$ é não é um domínio de fatoração única mas seus ideais são fatorados de maneira única. Antes disso, iremos enunciar algumas definições básicas de teoria dos anéis.

Definição 27. Uma função $\phi : \mathcal{R} \to \S$, onde $\mathcal{R}$ e $\S$ são anéis, é dita um homomorfismo de anéis se as seguintes condições são satisfeitas:

$\phi(a+b) = \phi(a) + \phi(b)$

$\phi(ab) = \phi(a)\phi(b)$ para quaisquer que sejam os $a, b \in \mathcal{R}$.

Para homomorfismo de anéis, o núcleo e a imagem são definidas de maneira usual, como em Álgebra Linear. Além disso, quando um homomorfismo de anéis é bijetor, diremos que este é um *Isormofismo*.

Lema 46. *Seja $\phi : \mathcal{R} \to \mathcal{S}$ um homomorfismo de anéis. Se $\mathcal{I}$ é um ideal de $\mathcal{I}$, então $\phi^{-1}(\mathcal{I})$ é um ideal de $\mathcal{R}$.*

Demonstração. Primeiro, verificaremos se $0_R \in \phi^{-1}(\mathcal{I})$. Note que

$$\phi(0_R) = \phi(0_R + 0_R)$$

$$\phi(0_R) = \phi(0_R) + \phi(0_R)$$

$$0_S = \phi(0_R)$$

Como $\mathcal{I}$ é ideal e $0_S = \phi(0_R)$, segue que $0_S = \phi(0_R) \in \phi^{-1}(\mathcal{I})$. Agora, tome $a, b \in \phi^{-1}(\mathcal{I})$. Precisamos verificar que $a - b \in \phi^{-1}(\mathcal{I})$. Como $a, b \in \phi^{-1}(\mathcal{I})$, então $\phi(a), \phi(b) \in \mathcal{I}$. Além

disso, como $\mathcal{I}$ é ideal, segue que $\phi(a) - \phi(b) \in \mathcal{I}$. Como ϕ é homomorfismo, então

$$\phi(a) + (-\phi(b)) = \phi(a - b).$$

Portanto, $\phi(a - b) \in \mathcal{I}$.
Para concluir a demonstração, basta verificar a lei de absorção. Ou seja, dado $s \in \phi^{-1}(\mathcal{I})$ e $a \in \mathcal{R}$, precisamos verificar que $sa \in \mathcal{I}$. Note que, como $s \in \phi^{-1}(\mathcal{I})$, temos que $\phi(s) \in \mathcal{I}$. Então, como $\mathcal{I}$ é ideal, segue que $\phi(s)\phi(a) \in \mathcal{I}$. Como ϕ é homomorfismo, segue que $\phi(s)\phi(a) = \phi(sa)$. Logo, $sa \in \phi^{-1}(\mathbb{I})$. ■

3.1 Domínios de Dedekind

Ainda não enunciamos formalmente, mas os domínio que possuem seus ideais fatorados de maneira única em produtos de ideais primos possuem uma nomenclatura definida, dada em homenagem ao matemático alemão Julius Wilhelm Richard Dedekind por *Domínios de Dedekind.*
Iremos definir alguns equivalências da definição para que facilite ao máximo a demonstração dos teoremas e corolários.

Definição 28. Um Domínio de Dedekind é um domínio de integridade $\mathcal{R}$, que não é corpo, tal que:

1. $\mathcal{R}$ é Noetheriano;
2. Todo ideal primo é maximal;
3. $\mathcal{R}$ é integralmente fechado sobre o corpo de frações.

3.2 $\mathbb{Z}[\sqrt{-5}]$

Teorema 47. *Em um domínio de ideais principais $\mathcal{R}$, quaisquer dois elementos $a, b \in \mathcal{R}$ sempre possuem um maior divisor comum.*

Demonstração. Considere o ideal (a, b). Como $\mathcal{R}$ é DIP, existe um elemento d tal que $(a, b) = (d)$. Logo, $a = dk$ e $b = dq$, com $k, q \in \mathcal{R}$. Logo, d é um divisor comum de a e b. Por outro lado, se $(d) = (a, b)$ implica em $d \in (a, b)$. Ou seja, $d = ax+by$ para certos $x, y \in$

$\mathcal{R}$. Então, se um elemento c divide a, b, então $c|ax$ e $c|by$. Logo, $c|ax + by = d$. Então, qualquer que seja um divisor comum c de a, b, temos que $c|d$. Logo, $d = mdc(a, b)$. ■

Corolário 48. *Em* $\mathbb{Z}[\sqrt{-5}]$*, os elementos* 6 *e* $2+2\sqrt{-5}$ *não possuem um máximo divisor comum.*

Demonstração. Note que em $\mathbb{Z}[\sqrt{-5}]$ podemos escrever o elemento 6 como

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Suponha por absurdo que exista um mdc entre 6 e $2+2\sqrt{-5}$. Denotaremos esse elemento por d. Logo, podemos escrever $6 = xd$ e $(2 + 2\sqrt{-5}) = yd$. Pela propriedade de norma dos inteiros quadráticos, temos que:

$$\mathcal{N}(6) = 36 = \mathcal{N}(xd) = \mathcal{N}(x)\mathcal{N}(d),$$

$$\mathcal{N}(2 + 2\sqrt{-5}) = 24 = N(yd) = \mathcal{N}(y)\mathcal{N}(d).$$

Disso nós temos que $\mathcal{N}(d)|36$ e $\mathcal{N}(d)|24$. Logo, os possíveis valores para $\mathcal{N}(d)$ são $1, 2, 3, 4, 6, 12$. Note que, $(1 + \sqrt{-5})$ divide 6 e $2 + 2\sqrt{-5}$. Logo, $(1 + \sqrt{-5})|d$. Portanto,

$$\mathcal{N}(1 + \sqrt{-5}) = 6 \mid \mathcal{N}(d).$$

Além disso, $2|6$ e $2|\left(2 + 2\sqrt{-5}\right)$. Logo,

$$\mathcal{N}(2) = 4 \mid \mathcal{N}(d).$$

Logo, a única possibilidade é que $\mathcal{N}(d) = 12$. Portanto, se $d = s + r\sqrt{-5}$, então $s^2 = 12+5r^2$ que não possui solução inteira. Logo, $6, 2(1+1\sqrt{-5})$ não possuem máximo divisor comum. ■

Com isso temos que $\mathbb{Z}[\sqrt{-5}]$ não é um domínio de ideais principais.

Lema 49. $\mathbb{Z}[\sqrt{-5}]$ *é Noetheriano.*

Demonstração. Considere o homomorfismo de anéis dado por

$$\phi\colon \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-5}]$$
$$p \mapsto p(\sqrt{-5}).$$

Note que $\phi(p) = 0$ implica em $p(\sqrt{-5}) = 0$. Logo, como o polinômio minimal de $\sqrt{-5}$ é $m(x) = x^2 + 5$, temos que $p(x) = m(x)q(x)$, onde $q(x) \in \mathbb{Z}[x]$. Consequentemente, $p(x) \in (x^2 + 5)$.
Além disso, considere u em $\mathbb{Z}[\sqrt{-5}]$ tal que $u = a + b\sqrt{-5}$. Ou seja, se tomarmos $p(x) = a + bx$, temos que

$$\phi(p) = p(\sqrt{5}) = a + b\sqrt{-5} = u.$$

Logo, o homomorfismo é sobrejetor. Portanto, pelo teorema do isomorfismo,

$$\mathbb{Z}\left[\sqrt{-5}\right] \simeq \frac{\mathbb{Z}\left[x\right]}{(x^2 + 5)}.$$

Como $\mathbb{Z}[x]$ é Noetheriano e $(x^2 + 5)$ é ideal, então segue que $\mathbb{Z}[\sqrt{-5}]$ é Noetheriano. ■

Lema 50. *Em $\mathbb{Z}[\sqrt{-5}]$ todo ideal primo é maximal.*

Demonstração. Considere $\mathcal{P}$ um ideal primo de $\mathbb{Z}[\sqrt{-5}]$. Logo, $\mathbb{Z}[\sqrt{-5}]/\mathcal{P}$ é um domínio de integridade finito. Considere

$$s, s^1, s^2, ... \in \mathbb{Z}[\sqrt{-5}]/\mathcal{P}.$$

Onde, s é um elemento não-nulo. Como o domínio é finito, então existe expoentes n e m tal que

$$s^n = s^m$$

Sem perda de generalidade, suponha que $n > m$. Portanto,

$$s^n - s^m = 0$$

$$s^m(s^{n-m} - 1) = 0$$

Como s é um domínio, então $s^m = 0$ ou $(s^{n-m} - 1) = 0$. Novamente por ser um domínio,

$s^m \neq 0$. Logo, $s^n - m = 1$. Portanto,

$$ss^{n-m-1} = 1.$$

Como tomamos s como um elemento fixo porém arbitrário, segue que $\mathbb{Z}[\sqrt{-5}]/\mathcal{P}$ é um corpo.
Concluimos assim que $\mathcal{P}$ é maximal. ■

Agora, construiremos um argumento que verifica qual a condição necessária e suficiente para que os inteiros quadráticos sejam integralmentes fechados sobre o corpo de frações $\mathbb{Q}[\sqrt{d}]$.
Considere $\alpha = \frac{a}{b} + \frac{p}{q}\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ com $mdc(a,b) = mdc(p,q) = 1$ e $q > 0, s > 0$. Se $p = 0$, então

$$\alpha \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{d}].$$

Suponha que $p \neq 0$. Então,

$$\left(\alpha - \frac{a}{b}\right)^2 = d\frac{p^2}{q^2}$$

$$\alpha^2 - 2\alpha\frac{a}{b} + \frac{a^2}{b^2} = d\frac{p^2}{q^2}$$

Logo, α é raíz do polinômio

$$m(x) = x^2 - 2\frac{a}{b}x + \frac{a^2}{b^2} - d\frac{p^2}{q^2}.$$

Para que $\mathbb{Z}[\sqrt{d}]$ seja integralmente fechado, devemos ter que cada coeficiente do polinômio $m(x)$ seja inteiro. Logo, $b|2a$. Como estamos assumindo que a e b são coprimos, temos que $b = 1$ ou $b = 2$. Se $b = 1$, então $m(x) = x^2 + 2ax + a^2 - d\frac{p^2}{q^2}$. Como a^2 é inteiro, segue que $d\frac{p^2}{q^2}$ é inteiro. Logo, $q^2|dp^2$. Na definição de inteiros quadráticos que adotamos, o elemento d deve ser um livre de quadrados. Logo, $q^2 = 1$ ou seja $q = \pm 1$. Portanto, $m(x) = x^2 + 2ax + a^2 - dp^2$. Concluimos então que $a + p\sqrt{d} = \alpha \in \mathbb{Z}[x]$.
Por outro lado, se $b = 2$, então

$$\frac{a^2}{4} - \frac{p^2 d}{q^2} = \frac{a^2q^2 - 4p^2d}{4q^2} \in \mathbb{Z}.$$

Logo, como $4p^2d$ é inteiro, segue que $4q^2|a^2q^2$. Em outra palavras, $4|a^2q^2$. Além disso, se

supomos que $b = 2$, então a é um número ímpar. Logo, $4|q^2$. Claramente q é um número par, ou seja, existe um inteiro s tal que $q = 2s$. Portanto:

$$\frac{a^2q^2 - 4p^2d}{4q^2} = \frac{4a^2s^2 - 4p^2d}{16s^2} \in \mathbb{Z}.$$

Como a é ímpar e p é ímpar, então $a^2 \equiv b^2 \equiv 1 \pmod 8$. Desde que $4|\,(a^2s^2 - p^2d)$, $a^2s^2 - p^2d \equiv s^2 - d \equiv 0 \pmod 4$ e d é livre de quadrados, então $d \equiv 1 \pmod 4$.
Logo, se tomarmos $d \equiv 1 \pmod 4$, $a = p = 1$ e $b = q = 2$, então temos que $\frac{1}{2} + \frac{1}{2} \in \mathbb{Q}(\sqrt{-5})$ mas não pertence à $\mathbb{Z}[\sqrt{-5}]$.
Ou seja, um critério para que um anel $\mathbb{Z}[\sqrt{d}]$ seja integralmente fechado, é que $d \not\equiv 1 \pmod 4$. Como no nosso caso $d = -5$ e $(-5) \not\equiv 1 \pmod 4$, segue que $\mathbb{Z}[\sqrt{-5}]$ é integralmente fechado. Concluímos assim que $\mathbb{Z}[\sqrt{-5}]$ é um Domínio de Dedekind.

Referências Bibliográficas

[1] CÁMPOLI, O. A. *A principal ideal domain that is not a Euclidean domain*, American Mathematical Monthly, vol. 95 no. 9. 1988. 868–871.

[2] GONÇALVES, A. *Introdução à Álgebra*. IMPA, Rio de Janeiro, 1979

[3] HUNGERFORD, T. W. *Abstract algebra: an introduction. Cengage Learning*, 2012.

[4] JARVIS, F. *Algebraic number theory.* New York: Springer, 2014. 298p.

[5] TRIFKOVIĆ, M. *Algebraic theory of quadratic numbers.* Springer, 2013.

[6] WILSON, R. A. *An example of a PID which is not a Euclidean domain. 2011.* Disponível em: <http://www.maths.qmul.ac.uk/ raw/MTH5100/PIDnotED.pdf>. Acesso em: 13 dez. 2018.