UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM MATEMÁTICA

Artur Assis Amorim

Teoria algébrica dos números aplicada a equações diofantinas não lineares

Juiz de Fora
2022

Artur Assis Amorim

Teoria algébrica dos números aplicada a equações diofantinas não lineares

Trabalho de conclusão de curso apresentado à Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Matemática.

Orientadora: Profa. Dra. Beatriz Casulari da Motta Ribeiro

Juiz de Fora

2022

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Amorim, Artur Assis.
Teoria algébrica dos números aplicada a equações diofantinas não lineares / Artur Assis Amorim. – 2022.
166 f.

Orientadora: Beatriz Casulari da Motta Ribeiro
Trabalho de Conclusão de Curso – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. Bacharelado em Matemática, 2022.

1. Teoria algébrica dos números. 2. Equações diofantinas não lineares. I. Ribeiro, Beatriz Casulari da Motta, orient. II. Título.

Artur Assis Amorim

Teoria algébrica dos números aplicada a equações diofantinas não lineares

Trabalho de conclusão de curso apresentado à Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Matemática.

Aprovada em 25 de Fevereiro de 2022

BANCA EXAMINADORA

Profa. Dra. Beatriz Casulari da Motta Ribeiro - Orientador
Universidade Federal de Juiz de Fora

Prof. Dr. Frederico Sercio Feitosa
Universidade Federal de Juiz de Fora

Profa. Dra. Tatiana Aparecida Gouveia
Universidade Federal de Juiz de Fora

Dedico este trabalho aos meus pais e à Regina.

AGRADECIMENTOS

Agradeço a meu pai, Glauker, por ter alimentado minha curiosidade e meu pensamento ao longo da vida, e a minha mãe, Gioconda, por sempre ter me incentivado a me dedicar e ter me ensinado coisas que fogem a razão.

Agradeço à professora Beatriz, com a qual a jornada de aprendizado começou anos antes de eu sequer sonhar em entrar na universidade. Seu conhecimento e experiência me tornaram um aluno, e uma pessoa, melhores. Agradeço ainda por sua paciência infinita e não-enumerável, da qual precisei quando os prazos se apertaram.

Agradeço à minha namorada de muitos anos, Isadora, que sempre serviu de inspiração e guia e por sempre ter me apoiado em meus estudos.

Agradeço a todos os professores e servidores que, direta ou indiretamente, fizeram parte da minha formação. Não há presente mais duradouro e útil que o conhecimento, o qual, graças a vocês, pude obter.

Agradeço à UFJF pela estrutura e pela excelência do ensino público, gratuito e inclusivo.

Por fim, agradeço a Regina. Seu impacto no mundo não pode ser medido pelo número de teoremas feitos, mas nenhum teorema, feito ou não, será capaz de medir o impacto que teve, no mundo e em mim. Foi extraordinária em vida, maior que o conjunto de suas partes e, mais ainda, foi minha segunda mãe. Viverá sempre em minha memória e meu coração.

"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratosquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet" - Pierre de Fermat

RESUMO

O estudo de equações diofantinas é um dos mais antigos dentro da matemática, tendo se relacionado historicamente com problemas importantes, como a determinação das ternas pitagóricas e o Último Teorema de Fermat. Mais recentemente, além de motivar avanços nas áreas de álgebra e na teoria dos números, equações diofantinas tem sido usadas dentro da criptografia, o que torna o estudo dessas equações cada vez mais importante.

Nesse trabalho, temos como objetivo estudar alguns métodos da teoria algébrica dos números para a resolução de equações diofantinas não-lineares. Para isso, estabeleceremos os conceitos básicos dessa área, como domínios de integridade e tipos especiais de domínios, no primeiro capítulo. Nos capítulos seguintes, desenvolvemos a teoria necessária para definir noções importantes, como ideais fracionários, normas de ideais e anéis de inteiros de um corpo de números algébricos, as quais confluem no sétimo capítulo para o estudo de domínios de Dedekind e da fatoração de ideais. Por fim, usamos dos resultados construídos ao longo do texto para estudar algumas equações diofantinas, fornecendo condições para a existência de soluções e, em certos casos, as determinando.

Palavras-chave: Teoria algébrica dos números. Equações diofantinas não lineares.

ABSTRACT

The study of diophantine equations is one of the oldest in mathematics, having been historically related to important problems, such as the determination of pythagorean triples and Fermat's Last Theorem. More recently, in addition to motivating advances in algebra and number theory, diophantine equations have been used within cryptography, which makes the study of these equations increasingly important.

In this work, we aim to study some methods of algebraic number theory for solving nonlinear diophantine equations. To do this, we will establish the basic concepts of this area, such as integral domains and special types of domains, in the first chapter. In the following chapters, we develop the theory necessary to define important notions, such as fractional ideals, norm of ideals and the ring of integers of an algebraic number field, which converge in the seventh chapter for the study of Dedekind domains and the factoring of ideals. Finally, we use the results constructed throughout the text to study some diophantine equations, providing conditions for the existence of solutions and, in certain cases, determining them.

Keywords: Algebraic number theory. Nonlinear diophantine equations.

LISTA DE SÍMBOLOS

(a, b)	Máximo divisor comum de a e b
$L(\alpha)$	Extensão simples de um corpo L adjuntado de α
$L(\alpha_1, ..., \alpha_n)$	Extensão múltipla de um corpo L adjuntado de $\alpha_1, ..., \alpha_n$
$\left(\frac{m}{p}\right)$	Símbolo de Legendre
$\langle\alpha\rangle$	Ideal gerado por α
A^B	Fecho inteiro de um domínio de integridade A em um domínio de integridade B
$\frac{M}{N}$	Conjunto quociente de M por N
$\mathbb{Z} + \mathbb{Z}\sqrt{n}$	O conjunto $\{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$
$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{n}}{2}\right)$	O conjunto $\left\{x + y\left(\frac{1+\sqrt{n}}{2}\right) \mid x, y \in \mathbb{Z}\right\}$
$p^\alpha \| b$	p^α divide b e $p^{\alpha+1}$ não divide b
PBO	Princípio da Boa Ordem
$\lfloor a \rfloor$	Maior inteiro menor ou igual que a.

SUMÁRIO

1 INTRODUÇÃO

A aritmética, precursora da teoria dos números, é uma das áreas mais antigas da matemática, depois da geometria. Dentro da infinidade de problemas nessa área, uma classe se destaca pela facilidade de encontrar nela problemas extremamente difíceis de serem resolvidos: as equações diofantinas. Desde a Grécia Antiga, somos capazes de resolver equações diofantinas lineares com duas variáveis, sendo estas estudadas atualmente em cursos introdutórios de teoria elementar dos números. Entretanto, a medida que o grau da equação e o número de variáveis crescem, não há um resultado geral que nos diga quais são as soluções ou se estas ao menos existem. Por exemplo, uma das equações diofantinas mais conhecidas é a equação $x^2 + y^2 = z^2$, expressão que aparece no Teorema de Pitágoras. A caracterização das soluções inteiras dessa equação é um resultado conhecido que nos fornece todas as triplas pitagóricas. Entretanto, um problema com enunciado semelhante, o qual difere apenas nos expoentes, é encontrar as soluções inteiras não-triviais da equação $x^n + y^n = z^n$, com n inteiro maior do que 2. Esse é o famoso Último Teorema de Fermat, o qual levou séculos para ser resolvido, e cuja demonstração fez uso da teoria algébrica dos números.

Isso nos leva à motivação por trás desse estudo. Na teoria elementar dos números, ao estudarmos equações diofantinas, tem-se algumas abordagens clássicas: a primeira delas é analisar os restos da equação na divisão por algum número. Tal procedimento costuma nos fornecer informações sobre os termos e, muitas vezes, é capaz de nos mostrar quando uma equação não tem solução. Esgotado esse método, recorremos então à uma ferramenta poderosa: o Teorema Fundamental da Aritmética. Com ele, tentamos reescrever os dois lados da equação como um produto de fatores (preferencialmente primos entre si), e utilizando da fatoração única como produto de primos, conseguimos obter muitas informações sobre os fatores desses produtos e, consequentemente, sobre possíveis soluções, sendo capazes de caracterizá-las em alguns casos. Note que, nessas abordagens, fizemos uso de alguns fatos: propriedades sobre primos, existência e cálculo do MDC, fatoração de termos e uso da fatoração única. O problema com essa abordagem é que nem sempre conseguimos reescrever a equação como um produto de ambos os lados da igualdade. De fato, considere a equação:

$$k = x^2 + 2y^2$$

com $k \in \mathbb{N}$. Nos inteiros, essa equação não pode ser facilmente fatorada em ambos os lados da igualdade. Entretanto, em $\mathbb{C}$, podemos escrever:

$$k = (x + y\sqrt{-2})(x - y\sqrt{-2})$$

Isso nos leva a estudar o conjunto $\{x+y\sqrt{-2} \mid x, y \in \mathbb{Z}\} \subset \mathbb{C}$, o qual veremos que se trata de um tipo de domínio cujas propriedades estudaremos a fundo. Esta é a ideia por trás da teoria algébrica dos números: generalizar os conceitos e propriedades conhecidas sobre

números inteiros para outros domínios. Esse processo, entretanto, não é tão simples. Como veremos, muitas das propriedades dos números inteiros não valem em certos domínios: irredutíveis e primos nem sempre coincidem, a fatoração em irredutíveis e o MDC nem sempre existem, e a fatoração, quando existe, nem sempre é única. Por isso, estudamos sob quais domínios tais condições valem. Ainda, desenvolvemos muitos capítulos de teoria para que possamos estudar outro tipo de domínio: os domínios de Dedekind. Nesses domínios, ainda que não haja a fatoração única de termos como produto de irredutíveis, veremos que esse problema pode ser superado fatorando os ideais gerados pelos elementos ao invés dos elementos em si. Esse método é extremamente poderoso e nos permite estudar uma classe muito maior de equações diofantinas do que aquelas que podem ser fatoradas em domínios de fatoração única.

Com essas técnicas, estudaremos, no último capítulo, diversas classes de equações, mostrando como podemos aplicar desde a teoria elementar dos números à fatoração de ideais para a resolução de equações diofantinas.

2 DOMÍNIOS EUCLIDIANOS, NOETHERIANOS E DE INTEGRIDADE

Começaremos este estudo dando algumas definições básicas de álgebra e teoria dos números, que serão fundamentais para estabelecer a linguagem que será usada, além das propriedades básicas para o desenvolvimento da teoria. Em particular, estudaremos nesse capítulo domínios de integridade, domínios de ideais principais, domínios Euclidianos, domínios de fatoração única e domínios Noetherianos, além de conceitos relacionados a esses domínios. Nos baseamos nos capítulos $1, 2$ e 3 de (1) para esta seção.

2.1 DOMÍNIOS DE INTEGRIDADE

Iniciaremos com o estudo de domínios de integridade, os quais tem como objetivo generalizar as propriedades operacionais dos números inteiros.

Definição 1 (Domínio de Integridade)**.** *Um domínio de integridade é um anel comutativo D com unidade e sem divisores de 0. Se, para todo $a \in D$, $a \neq 0$, existe $b \in D$ com $ab = 1$, então D é chamado de corpo.*

Vejamos exemplos de domínios de integridade que serão utilizaremos no texto:

Exemplo 1. *$\mathbb{Z}$ é um domínio de integridade.*

Definição 2 (Inteiro livre de quadrados)**.** *Seja $l \in \mathbb{Z} \setminus \{0\}$. Dizemos que l é livre de quadrados se, para todo $d \in \mathbb{Z}$, $d^2 \mid l$ implicar em $d \in \{-1, 1\}$.*

Exemplo 2. *Sejam $m, n \in \mathbb{Z}$ livres de quadrados, com $m \equiv 1 \pmod 4$. Então:*

$$\mathbb{Z} + \mathbb{Z}\sqrt{n} = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$
$$\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) = \left\{a + b\left(\frac{1+\sqrt{m}}{2}\right) \mid a, b \in \mathbb{Z}\right\}$$

com as operações $+$ e $\times$ herdadas de $\mathbb{C}$ são domínios de integridade. De fato, temos $\mathbb{Z} + \mathbb{Z}\sqrt{n}, \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \subset \mathbb{C}$, donde $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ e $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ satisfazem as propriedades da soma ser associativa, comutativa e distributiva com relação ao produto, o qual é associativo e comutativo. Ainda, como $\mathbb{C}$ é corpo, vale que $\mathbb{C}$ (e, por consequência, $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ e $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$) não possui divisores de 0. Devemos então mostrar que $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ e $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ são fechados para a soma e para o produto, que 0 e 1 pertencem a ambos os conjuntos, e que o inverso aditivo de cada elemento desses conjuntos também está no respectivo conjunto. Mostremos que tais afirmações valem:

- $0, 1 \in \mathbb{Z} + \mathbb{Z}\sqrt{n}, \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right)$: *Por definição, tomando* $a = 0$ *e* $b = 0$, *temos:*

$$a + b\sqrt{n} = 0 + 0\sqrt{n} = 0 \in \mathbb{Z} + \mathbb{Z}\sqrt{n}$$
$$a + b\left(\frac{1+\sqrt{m}}{2}\right) = 0 + 0\left(\frac{1+\sqrt{m}}{2}\right) = 0 \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

Analogamente, tomando $a = 1$ *e* $b = 0$, *temos:*

$$a + b\sqrt{n} = 1 + 0\sqrt{n} = 1 \in \mathbb{Z} + \mathbb{Z}\sqrt{n}$$
$$a + b\left(\frac{1+\sqrt{m}}{2}\right) = 1 + 0\left(\frac{1+\sqrt{m}}{2}\right) = 1 \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

- $\mathbb{Z} + \mathbb{Z}\sqrt{n}$ *e* $\mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right)$ *são fechados para a soma e para o produto: Sejam* $u, v \in \mathbb{Z} + \mathbb{Z}\sqrt{n}$ *e* $x, y \in \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right)$. *Então, existem* $a, b, c, d, e, f, g, h \in \mathbb{Z}$ *tais que:*

$$u = a + b\sqrt{n}$$
$$v = c + d\sqrt{n}$$
$$x = e + f\left(\frac{1+\sqrt{m}}{2}\right)$$
$$y = g + h\left(\frac{1+\sqrt{m}}{2}\right)$$

Então:

$$u + v = \left(a + b\sqrt{n}\right) + \left(c + d\sqrt{n}\right) = (a + c) + (b + d)\sqrt{n} \in \mathbb{Z} + \mathbb{Z}\sqrt{n}$$
$$x + y = \left(e + f\left(\frac{1+\sqrt{m}}{2}\right)\right) + \left(g + h\left(\frac{1+\sqrt{m}}{2}\right)\right) =$$
$$= (e + g) + (f + h)\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

uma vez que $a + c, b + d, e + g, f + h \in \mathbb{Z}$ *(pois* $\mathbb{Z}$ *é domínio de integridade). Ainda, como* $m \equiv 1 \pmod 4$, *temos que* $m + 1 \equiv 2 \pmod 4$, *donde existe* $k \in \mathbb{Z}$ *tal que*

$m+1 = 4k+2$. *Com isso:*

$$uv = \left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right) = (ac+bdn)+(ad+bc)\sqrt{n} \in \mathbb{Z}+\mathbb{Z}\sqrt{n}$$

$$xy = \left(e+f\left(\frac{1+\sqrt{m}}{2}\right)\right)+\left(g+h\left(\frac{1+\sqrt{m}}{2}\right)\right) =$$

$$= (eg)+(eh+fg)\left(\frac{1+\sqrt{m}}{2}\right)+fh\left(\frac{1+\sqrt{m}}{2}\right)^2 =$$

$$= (eg)+(eh+fg)\left(\frac{1+\sqrt{m}}{2}\right)+fh\left(\frac{1+2\sqrt{m}+m}{4}\right) =$$

$$= (eg)+(eh+fg)\left(\frac{1+\sqrt{m}}{2}\right)+fh\left(\frac{4k+2+2\sqrt{m}}{4}\right) =$$

$$= (eg)+(eh+fg)\left(\frac{1+\sqrt{m}}{2}\right)+fh\left(k+\frac{1+\sqrt{m}}{2}\right) =$$

$$= (eg+fhk)+(eh+fg+fh)\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

uma vez que $ac+bdn, ad+bc, eg+fhk, eh+fg+fh \in \mathbb{Z}$ *(pois* $\mathbb{Z}$ *é domínio de integridade). Logo,* $\mathbb{Z}+\mathbb{Z}\sqrt{n}$ *e* $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ *são fechados para soma e para o produto.*

- $\mathbb{Z}+\mathbb{Z}\sqrt{n}$ *e* $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ *contém os inversos aditivos de seus elementos: Sejam* $u \in \mathbb{Z}+\mathbb{Z}\sqrt{n}$ *e* $x \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$*. Então, existem* $a, b, c, d \in \mathbb{Z}$ *tais que:*

$$u = a+b\sqrt{n}$$
$$x = c+d\left(\frac{1+\sqrt{m}}{2}\right)$$

Então, como $-a, -b, -c, -d \in \mathbb{Z}$*, temos que:*

$$-a-b\sqrt{n} = -(a+b\sqrt{n}) = -u \in \mathbb{Z}+\mathbb{Z}\sqrt{n}$$
$$-c-d\left(\frac{1+\sqrt{m}}{2}\right) = -\left(c+d\left(\frac{1+\sqrt{m}}{2}\right)\right) = -x \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$$

Com isso, vemos que $\mathbb{Z}+\mathbb{Z}\sqrt{n}$ *e* $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ *são domínios de integridade.*

Exemplo 3. *Sejam* D *um domínio de integridade e* $D[x]$ *o anel de polinômios na variável* x *com coeficientes em* D*.* $D[x]$ *é um domínio de integridade.*

Daremos agora a definição de um divisor em domínios de integridade, de maneira análoga à como é feito para números inteiros.

Definição 3 (Divisor)**.** *Sejam D um domínio de integridade e $a, b \in D$. Dizemos que a é divisor de b (ou que a divide b) se existe $c \in D$ tal que $b = ac$. Caso a seja divisor de b, escrevemos $a \mid b$. Do contrário, escrevemos $a \nmid b$.*

Da mesma forma, podemos generalizar o conceito de unidade para domínios de integridade.

Definição 4 (Unidade)**.** *Um elemento a de um domínio de integridade D é chamado de unidade se $a \mid 1$. O conjunto das unidades de D é denotado por $U(D)$.*

Nos números naturais, as afirmações $a \mid b$ e $b \mid a$ implicam em $a = b$. Tal fato já não é válido em $\mathbb{Z}$, uma vez que $-1 \mid 1$, $1 \mid -1$ e $-1 \neq 1$. Assim como nos inteiros, em domínios de integridade $a \mid b$ e $b \mid a$ não implicam, no geral, que $a = b$. Apesar disso, o fato de a e b dividirem um ao outro ainda trás propriedades importantes, e por isso é interessante caracterizar esses elementos.

Definição 5 (Associados)**.** *Sejam $a, b \in D$, $a, b \neq 0$, sendo D um domínio de integridade. Dizemos que a e b são associados, e escrevemos $a \sim b$, caso $a \mid b$ e $b \mid a$. Se a e b não forem associados, escrevemos $a \not\sim b$.*

Mostremos uma propriedade interessante de elementos associados.

Proposição 1. *Sejam D um domínio de integridade e $a, b, c \in D$, com $a = bc$. Então $c \in U(D) \Leftrightarrow a \sim b$.*

Demonstração. ($\Rightarrow$) Se $c \in U(D)$, existe $r \in D$ tal que $cr = 1$. Assim, como $a = bc$, temos $b \mid a$. Ainda, $ar = b(cr) = b \Rightarrow a \mid b$. Logo, $a \sim b$.
($\Leftarrow$) Como $a \sim b$, temos $a \mid b$. Logo, existe $r \in D$ tal que $b = ar \Rightarrow a = bc = acr$. Ainda, como $a \sim b$, temos por definição que $a, b \neq 0$, donde $acr = a$ implica em $cr = 1$. Assim, $c \mid 1$, donde $c \in U(D)$. □

Daremos agora a primeira definição que difere daquelas usuais para números inteiros. Em $\mathbb{Z}$, um número primo é, também, irredutível, no sentido que definiremos mais adiante. Tal fato, entretanto, não é verdade para domínios de integridade no geral.

Definição 6 (Irredutível)**.** *Seja $a \in D$, D um domínio de integridade, com $a \neq 0, 1$. Dizemos que a é irredutível se $a = bc$, com $b, c \in D \Rightarrow b \in U(D)$ ou $c \in U(D)$. Um elemento a de D que não é irredutível é dito redutível.*

Poderíamos reescrever a definição acima da seguinte forma: Seja $a \in D$, D um domínio de integridade, com $a \neq 0, 1$. Dizemos que a é irredutível se $a = bc$, com $b, c \in D \Rightarrow b \sim a$ ou $c \sim a$.

De fato, se a é irredutível, então $a = bc$, com $b, c \in D \Rightarrow b \in U(D)$ ou $c \in U(D)$. Se $b \in U(D)$, então existe $r \in D$ tal que $br = 1$. Assim, $a = bc \Rightarrow c \mid a$ e $ra = (rb)c = c \Rightarrow a \mid c$. Logo, $c \sim a$. Analogamente, se $c \in U(D)$, então existe $s \in D$ tal que $cs = 1$. Assim, $a = bc \Rightarrow b \mid a$ e $as = b(cs) = b \Rightarrow a \mid b$. Logo, $b \sim a$. Portanto, a irredutível e $a = bc$, com $b, c \in D \Rightarrow b \sim a$ ou $c \sim a$.

Por outro lado, seja $a \in D$, com D domínio de integridade, $a \neq 0, 1$ e tal que $a = bc$, com $b, c \in D \Rightarrow b \sim a$ ou $c \sim a$. Dados $b, c \in D$, com $a = bc$, temos $b \sim a$ ou $c \sim a \Rightarrow a \mid b$ ou $a \mid c \Rightarrow$ existem $r, s \in D$ tais que $b = ar$ ou $c = as \Rightarrow a = bc = a(rc)$ ou $a = bc = a(bs) \Rightarrow rc = 1$ ou $bs = 1 \Rightarrow c \mid 1$ ou $b \mid 1 \Rightarrow b \in U(D)$ ou $c \in U(D)$. Logo, a é irredutível.

Mostremos agora que os elementos irredutíveis de um domínio de integridade satisfazem uma das propriedades características dos números primos nos inteiros.

Proposição 2. *Sejam D um domínio de integridade e $a \in D$ irredutível. Se $b \in D$ e $b \mid a$, então $b \in U(D)$ ou $b \sim a$.*

Demonstração. Se $b \in D$ e $b \mid a$, existe $c \in D$ tal que $a = bc$. Como a é irredutível, temos $b \in U(D)$ ou $c \in U(D)$. Se $b \notin U(D)$, temos $c \in U(D) \Rightarrow a \sim b$.
Assim, $b \in U(D)$ ou $b \sim a$. □

Daremos agora a definição de um elemento primo em um domínio de integridade (generalizando outra propriedade dos números primos) e veremos que, em um domínio de integridade, não é sempre verdade que um elemento irredutível é primo.

Definição 7 (Primo)**.** *Seja $p \in D$, D um domínio de integridade, com $p \neq 0, 1$. Dizemos que p é primo se $p \mid bc$, com $b, c \in D$ então $p \mid b$ ou $p \mid c$.*

Pelo que mostramos, $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ é um domínio de integridade. Mostraremos que $2 \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ é irredutível em $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$, mas não é primo nesse domínio. De fato, sejam $a, b, c, d \in \mathbb{Z}$ tais que:

$$\left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = (ac - 5bd) + (ad + cb)\sqrt{-5} = 2$$

Então:

$$\begin{cases} ac - 5bd = 2 \\ ad + cb = 0 \end{cases}$$

Com isso, temos $acd + c^2b = 0$, donde:

$$2d = d(ac - 5bd) = acd - 5bd^2 = -c^2b - 5bd^2 = -b(c^2 + 5d^2)$$

Da mesma forma, temos $ad^2 + cbd = 0$, donde:

$$2c = ac^2 - 5cbd = ac^2 + 5ad^2 = a(c^2 + 5d^2)$$

Dessa forma, segue que:

$$\begin{aligned} 2(c+d\sqrt{-5}) = 2c+2d\sqrt{-5} &= a(c^2+5d^2) - b\sqrt{-5}(c^2+5d^2) = \\ &= (a-b\sqrt{-5})(c^2+5d^2) = (a-b\sqrt{-5})(c+d\sqrt{-5})(c-d\sqrt{-5}) \end{aligned}$$

Como $c+d\sqrt{-5} \neq 0$ (pois nesse caso teríamos $2=0$, o que é falso), segue que:

$$2 = (a-b\sqrt{-5})(c-d\sqrt{-5})$$

Portanto:

$$4 = 2\times 2 = (a+b\sqrt{-5})(c+d\sqrt{-5})(a-b\sqrt{-5})(c-d\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2)$$

Note que $a^2+5b^2, c^2+5d^2 \in \mathbb{N}$. Segue então que $a^2+5b^2, c^2+5d^2 \mid 4$. Analisemos então as possibilidades:

- Caso $a^2+5b^2=1$: Nesse caso, como $a^2+5b^2 \geq 5b^2$, se tivermos $b\neq 0$, teremos $1 = a^2+5b^2 \geq 5$, o que é um absurdo. Logo, $b=0$ e $a^2=1$, donde $a=\pm 1$. Entretanto, note que $1, -1 \mid 1$, donde $a+b\sqrt{-5} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{-5})$.
- Caso $a^2+5b^2=2$: Note que $b\neq 0$ implica em $2 = a^2+5b^2 \geq 5b^2 \geq 5$, o que é um absurdo. Logo, $a^2=2$, donde $a=\pm\sqrt{2} \notin \mathbb{Z}$, o que é impossível.
- Caso $a^2+5b^2=4$: Nesse caso, $c^2+5d^2=1$, donde, pelo primeiro caso, temos $c+d\sqrt{-5} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{-5})$.

Portanto, $a+b\sqrt{-5} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{-5})$ ou $c+d\sqrt{-5} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{-5})$, donde 2 é irredutível em $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.

Mostremos agora que 2 não é primo em $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$. De fato, $1+\sqrt{-5}, 1-\sqrt{-5} \in \mathbb{Z}+\mathbb{Z}\sqrt{-5}$ e:

$$2 \mid 6 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$$

Mas $\dfrac{1+\sqrt{-5}}{2} = \dfrac{1}{2}+\dfrac{1}{2}\sqrt{-5} \notin \mathbb{Z}+\mathbb{Z}\sqrt{-5}$ e $\dfrac{1-\sqrt{-5}}{2} = \dfrac{1}{2}-\dfrac{1}{2}\sqrt{-5} \notin \mathbb{Z}+\mathbb{Z}\sqrt{-5}$. Logo, 2 não é primo em $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$.

Com essas considerações, vemos que os conceitos de elemento irredutível e elemento primo em domínios Euclidianos não necessariamente coincidem, como ocorre em $\mathbb{Z}$. É interessante, então, estudar como estes conceitos estão relacionados. Isso nos leva ao seguinte resultado:

Teorema 1. *Em um domínio de integridade D, todo primo é irredutível.*

Demonstração. Sejam $p \in D$ um primo e $p = ab$, $a, b \in D$. Assim, $p \mid ab$ e, sendo p primo, temos que $p \mid a$ ou $p \mid b$. Sem perda de generalidade, podemos supor

que $p \mid a$. Assim, $\frac{a}{p} \in D$ e $\frac{a}{p} \times b = \frac{ab}{p} = \frac{p}{p} = 1$, donde $b \mid 1 \Rightarrow b \in U(D)$. Portanto, $p \in D$ primo e $p = ab$, com $a, b \in D$, donde $a \in U(D)$ ou $b \in U(D) \Rightarrow p$ é irredutível. □

Podemos nos perguntar em quais casos a recíproca é verdadeira. Veremos, mais a frente, algumas condições que podemos exigir sobre o domínio de integridade de forma a fazê-la verdade. Para isso, devemos definir alguns outros conceitos:

Definição 8 (Ideal)**.** *Um ideal I de um domínio de integridade D é um subconjunto não-vazio de D com as seguintes propriedades:*

- $a, b \in I \Rightarrow a + b \in I$.
- $a \in I, r \in D \Rightarrow ra \in I$.

Se $I \neq D, \{0\}$, I é dito um ideal próprio de D.

Definição 9 (Ideal Principal)**.** *Um ideal I de um domínio de integridade D é dito um ideal principal se existe um elemento $a \in I$ tal que $I = \langle a \rangle$, em que $\langle a \rangle = \{ra;\ r \in D\}$. Neste caso, a é dito um gerador do ideal I.*

Podemos generalizar a notação da definição anterior. Seja $n \in \mathbb{N}^*$. Dados $a_1, a_2, ..., a_n \in D$, considere $\langle a_1, a_2, ..., a_n \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, r_2, ..., r_n \in D \right\}$ o conjunto das combinações lineares de $a_1, a_2, ..., a_n$. Vamos mostrar que $\langle a_1, a_2, ..., a_n \rangle$ é um ideal de D:

- $a, b \in \langle a_1, a_2, ..., a_n \rangle \Rightarrow a + b \in \langle a_1, a_2, ..., a_n \rangle$: De fato, dados $a, b \in \langle a_1, a_2, ..., a_n \rangle$, temos $a = \sum_{i=1}^{n} r_i a_i$ e $b = \sum_{i=1}^{n} s_i a_i$, com $r_1, r_2, ..., r_n, s_1, s_2, ..., s_n \in D$. Sendo $c_i = r_i + s_i \in D$, para $i = 1, 2, ..., n$, temos $a + b = \sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{n} s_i a_i = \sum_{i=1}^{n} (r_i + s_i) a_i = \sum_{i=1}^{n} c_i a_i$, $c_1, c_2, ..., c_n \in D \Rightarrow a + b \in \langle a_1, a_2, ..., a_n \rangle$.
- $a \in \langle a_1, a_2, ..., a_n \rangle$, $r \in D \Rightarrow ar \in \langle a_1, a_2, ..., a_n \rangle$: Dados $a \in \langle a_1, a_2, ..., a_n \rangle$ e $r \in D$, temos $a = \sum_{i=1}^{n} r_i a_i$. Sendo $R_i = r r_i \in D$, para $i = 1, 2, ..., n$, segue que $ra = r \sum_{i=1}^{n} r_i a_i = \sum_{i=1}^{n} r r_i a_i = \sum_{i=1}^{n} R_i a_i$, com $R_1, R_2, ..., R_n \in D \Rightarrow ra \in \langle a_1, a_2, ..., a_n \rangle$.

Por fim, note que $a_1 = \sum_{i=1}^{n} R_i a_i$, com $R_1 = 1$ e $R_i = 0$ para $i = 2, ..., n$, donde $a_1 \in \langle a_1, a_2, ..., a_n \rangle \Rightarrow \langle a_1, a_2, ..., a_n \rangle \neq \emptyset$. Portanto, para todo $n \in \mathbb{N}^*$ e para todo $\{a_1, a_2, ..., a_n\} \subset D$ tem-se que $\langle a_1, a_2, ..., a_n \rangle$ é um ideal de D.

Prosseguimos agora provando algumas propriedades sobre ideais, as quais nos serão úteis mais a frente.

Proposição 3. *Sejam D um domínio de integridade e $a, b \in D$. São equivalentes:*

1. $\langle a \rangle \subset \langle b \rangle$.
2. $b \mid a$.
3. $a \in \langle b \rangle$.

Demonstração. $(1 \Rightarrow 2)$ Como $a \in \langle a \rangle \subset \langle b \rangle$, temos $a = bs$, $s \in D \Rightarrow b \mid a$.
$(2 \Rightarrow 3)$ Como $b \mid a$, existe $r \in D$ tal que $a = br$, donde $a \in \langle b \rangle$.
$(3 \Rightarrow 1)$ Como $a \in \langle b \rangle$, existe $r \in D$ tal que $a = br$. Dado $c \in \langle a \rangle$, temos $c = as$, $s \in D \Rightarrow c = (br)s = b(rs)$, $rs \in D \Rightarrow c \in \langle b \rangle$. Assim, $\langle a \rangle \subset \langle b \rangle$. □

Proposição 4. *Sejam D um domínio de integridade, I um ideal de D e $a \in D$. Temos $a \in I \Leftrightarrow \langle a \rangle \subset I$.*

Demonstração. $(\Rightarrow)$ Dado $b \in \langle a \rangle$, existe $r \in D$ tal que $b = ra$. Como $a \in I$ e $r \in D$, temos $ra = b \in I$. Logo, $\langle a \rangle \subset I$.
$(\Leftarrow)$ Como $\langle a \rangle \subset I$ e $a \in \langle a \rangle$, temos $a \in I$. □

Teorema 2. *Sejam D um domínio de integridade e $a, b \in D^* = D \setminus \{0\}$. Então $\langle a \rangle = \langle b \rangle$ se, e somente se, $\dfrac{a}{b} \in U(D)$.*

Demonstração. $(\Rightarrow)$ Se $\langle a \rangle = \langle b \rangle$, temos que existem $r, s \in D$ tais que $a = br$ e $b = as$. Assim, $a = br = (as)r = a(sr)$ e $a \neq 0 \Rightarrow sr = 1 \Rightarrow r \mid 1 \Rightarrow r = \dfrac{a}{b} \in U(D)$.
$(\Leftarrow)$ Se $\dfrac{a}{b} \in U(D)$, existe $r \in D$ tal que $\dfrac{a}{b} \times r = 1 \Rightarrow b = ar \Rightarrow a \mid b \Rightarrow \langle b \rangle \subset \langle a \rangle$. Por outro lado, como $\dfrac{a}{b}$ está bem definido (isto é, $\dfrac{a}{b} \in D$), temos $a = \dfrac{a}{b} \times b \Rightarrow b \mid a \Rightarrow \langle a \rangle \subset \langle b \rangle$. Logo, $\langle a \rangle = \langle b \rangle$. □

Em particular, temos que se $a \in D^*$, $b \in D$ e $\langle a \rangle = \langle b \rangle$, então $b \in D^*$ e $a \sim b$. De fato, $b = 0$ implica em $\langle b \rangle = \{0\}$ e $a \notin \{0\}$, donde não podemos ter $\langle a \rangle = \langle b \rangle$. Assim, $\langle a \rangle = \langle b \rangle$ e segue que existe $c \in U(D)$ tal que $a = bc$. Analogamente, se $a = 0$ e $b \in D$ tal que $\langle a \rangle = \langle b \rangle$, temos $b = 0$. De fato, $b \neq 0$ implica em $b \notin \{0\} = \langle a \rangle$. Logo, $b = 0$ e então existe $c \in U(D)$ tal que $a = bc$. Com essas considerações, temos o seguinte corolário:

Corolário 1. *Sejam D um domínio de integridade e $a, b \in D$. Então, $\langle a \rangle = \langle b \rangle$ se, e somente se, existe $u \in U(D)$ tal que $a = bu$.*

Demonstração. Pelas considerações anteriores, sabemos que $\langle a \rangle = \langle b \rangle$ implica que existe $u \in U(D)$ tal que $a = bu$. Reciprocamente, se existe $u \in U(D)$ tal que $a = bu$, temos pela Proposição 3 que $\langle a \rangle \subset \langle b \rangle$. Como $u \in U(D)$, existe $u^{-1} \in U(D)$ tal que $u^{-1}a = b$, donde, pela Proposição 3, segue que $\langle b \rangle \subset \langle a \rangle$. Com isso, temos $\langle a \rangle = \langle b \rangle$ e o resultado segue. □

2.2 DOMÍNIOS DE IDEAIS PRINCIPAIS

Definição 10 (Domínio de Ideais Principais)**.** *Um domínio de integridade D é chamado domínio de ideais principais se todo ideal de D é principal.*

O primeiro exemplo de um domínio de ideais principais é o $\mathbb{Z}$:

Teorema 3. *$\mathbb{Z}$ é um domínio de ideais principais.*

Demonstração. Seja I um ideal de $\mathbb{Z}$. Se $I = \{0\}$ então $I = \langle 0\rangle$, donde I é um ideal principal. Se $I \neq \{0\}$, então existe $a \in I$, $a \neq 0$. Considere o conjunto $S = \{b \in I; b > 0\}$. Como $a \neq 0$, temos $a > 0$ ou $-a > 0$. Como $a \in I$, $(-1) \in \mathbb{Z} \Rightarrow -a \in I$. Assim, $|a| \in I$ e $|a| > 0$, donde $|a| \in S \Rightarrow S \neq \emptyset$. Como $S \subset \mathbb{N}$, temos pelo PBO que existe $s = min\ S$. Seja $b \in I$. Como $s > 0$, temos pelo algoritmo de Euclides que existem $q, r \in \mathbb{Z}$, com $0 \leq r < s$, tais que $b = qs + r$. Suponha que $r \neq 0$. Então $s > r = b - qs > 0$. Como $s \in I, -q \in \mathbb{Z}$, temos $-qs \in I$. Ainda, $b, -qs \in I$ implica em $b + (-qs) = b - qs = r \in I$. Assim, $r \in I$ e $r > 0 \Rightarrow r \in S$ e $r < s = min\ S$, o que é um absurdo. Logo, devemos ter $r = 0$, donde $b = qs \Rightarrow b \in \langle s\rangle$. Dessa forma, $I \subset \langle s\rangle$. Sendo $s \in S \subset I$, temos $\langle s\rangle \subset I$. Portanto, $I = \langle s\rangle$ e I é um ideal principal.
Assim, $\mathbb{Z}$ é um domínio de ideais principais. □

As propriedades dos domínios de ideais principais nos permitem demonstrar muitos resultados que são verdade em $\mathbb{Z}$, mas não são verdade para domínios de integridade em geral. Em particular, mostraremos que a recíproca do Teorema 1 vale para domínios de ideais principais.

Teorema 4. *Em um domínio de ideais principais, todo irredutível é primo.*

Demonstração. Seja p um irredutível em um domínio de ideais principais D. Sejam $a, b \in D$ tais que $p = ab$. Se $p \nmid a$, considere $I = \langle p, a\rangle$ um ideal de D. Como D é um domínio de ideais principais, existe $r \in D$ tal que $I = \langle r\rangle$. Como $a, p \in I = \langle r\rangle$, temos $r \mid a$ e $r \mid p$. Se $p \mid r$ então $p \mid a$, o que é um absurdo. Assim, $p \nmid r \Rightarrow p \not\sim r$. Como $r \mid p$ e p é irredutível, segue que $r \in U(D)$. Assim, existe $d \in D$ tal que $rd = 1$. Sendo $r \in \langle p, a\rangle$, existem $x, y \in D$ tais que:

$$r = ax + py$$
$$1 = rd = axd + pyd$$
$$b = abxd + pbyd = pxd + pbyd = p(xd + byd)$$

Como $xd + byd \in D$, temos que $p \mid b$. Assim, $p|a$ ou $p|b \Rightarrow p$ é primo. □

Como uma consequência dos Teoremas 1 e 4, temos:

Teorema 5. *Em um domínio de ideais principais, um elemento é irredutível se, e somente se, é primo.*

Este resultado nos mostra que, em domínios de ideais principais, os elementos primos e os elementos irredutíveis coincidem, tal como ocorre em $\mathbb{Z}$. Vejamos outra definição dos números inteiros que é possível generalizar para domínios de ideais principais.

Definição 11 (Máximo Divisor Comum)**.** *Sejam D um domínio de ideais principais e $\{a_1, a_2, ..., a_n\} \subset D$. Então $\langle a_1, a_2, ..., a_n\rangle$ é um ideal principal de D. Um gerador deste ideal é chamado de máximo divisor comum (MDC) de $a_1, a_2, ..., a_n$.*

Note que o gerador do ideal $\langle a_1, a_2, ..., a_n\rangle$ não está, necessariamente, unicamente determinado. Na verdade, mesmo em $\mathbb{Z}$, temos $\langle a\rangle = \langle -a\rangle$. Entretanto, sabemos pelo Corolário 1 que dois geradores $a, b \in D$ do ideal acima satisfazem $a = bu$, com $u \in U(D)$. Assim, o MDC de elementos de D está unicamente determinado a menos de unidade.

Definição 12 (Símbolo de Legendre)**.** *Sejam $p > 2$ um número primo e $a \in \mathbb{Z}$. Definimos o símbolo de Legendre como sendo:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } p \nmid a \text{ e existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv a \pmod{p} \\ 0, & \text{se } p \mid a \\ -1, & \text{caso contrário} \end{cases}$$

Provaremos agora um resultado que nos dá informações importantes para o estudo de equações diofantinas.

Teorema 6. *Seja m um inteiro que não é quadrado perfeito tal que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é um domínio de ideais principais. Considere p um primo ímpar tal que $\left(\frac{m}{p}\right) = 1$. Então existem $u, v \in \mathbb{Z}$ tais que:*

- *$p = u^2 - mv^2$, caso $m < 0$ ou $m > 0$ e existam $T, U \in \mathbb{Z}$ tais que $T^2 - mU^2 = -1$.*
- *$p = u^2 - mv^2$ ou $p = mv^2 - u^2$, caso $m > 0$ e não existam $T, U \in \mathbb{Z}$ tais que $T^2 - mU^2 = -1$.*

Demonstração. Como $\left(\frac{m}{p}\right) = 1$, existe $x \in \mathbb{Z}$ tal que $x^2 \equiv m \pmod{p}$. Dessa forma, $p \mid (x - \sqrt{m})(x + \sqrt{m})$ em $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Como $\frac{x}{p} + \frac{\sqrt{m}}{p}, \frac{x}{p} - \frac{\sqrt{m}}{p} \notin \mathbb{Z} + \mathbb{Z}\sqrt{m}$, temos que $p \nmid x \pm \sqrt{m}$. Consequentemente, temos que p não é primo em $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. Mas $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é um domínio de ideais principais. Pelo teorema anterior, temos p redutível. Assim, existem $u, v, w, t \in \mathbb{Z}$ tais que:

$$p = (u + v\sqrt{m})(w + t\sqrt{m}) = (uw + tvm) + (ut + vw)\sqrt{m} \tag{2.1}$$

Com $u+v\sqrt{m}, w+t\sqrt{m} \notin U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$. De (2.1) podemos concluir que:

$$uw+tvm = p \text{ e } ut+vw = 0$$

Assim:

$$p^2 = (uw+tvm)^2 = (uw+tvm)^2 - m(ut+vw)^2$$
$$p^2 = u^2w^2 + 2uwtvm + t^2v^2m^2 - mu^2t^2 - 2uwtvm - mv^2w^2$$
$$p^2 = u^2w^2 + t^2v^2m^2 - mu^2t^2 - mv^2w^2$$
$$p^2 = (u^2-mv^2)(w^2-mt^2)$$

Como $m, u, w, v, t \in \mathbb{Z}$, temos $u^2-mv^2, w^2-mt^2 \in \mathbb{Z}$. Ainda, como $u+v\sqrt{m}, w+t\sqrt{m} \notin U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$, temos $u^2-mv^2, w^2-mt^2 \neq \pm 1$. Assim, sendo p um primo, devemos ter $p = u^2-mv^2 = w^2-mt^2$ ou $-p = u^2-mv^2 = w^2-mt^2$. Assim, existem inteiros u, v tais que $p = u^2-mv^2$ ou $p = -(u^2-mv^2)$.

Se $m < 0$, então $u^2-mv^2 > 0$, donde devemos ter $p = u^2-mv^2$.

Se $m > 0$, então $p = -(u^2-mv^2)$. Caso existam inteiros T e U tais que $T^2-mU^2 = -1$ então tomando $u' = Tu+mUv$, $v' = Uu+Tv$ temos $u'^2-mv'^2 = (Tu+mUv)^2 - m(Uu+Tv)^2 = T^2u^2 + 2TumUv + m^2U^2v^2 - mU^2u^2 - 2mUuTv - mT^2v^2 = T^2u^2 + m^2U^2v^2 - mU^2u^2 - mT^2v^2 = T^2(u^2-mv^2) - mU^2(u^2-mv^2) = (T^2-mU^2)(u^2-mv^2) = -(u^2-mv^2) = p$, donde existem $u', v' \in \mathbb{Z}$ tais que $p = u'^2-mv'^2$. □

Um resultado análogo vale para domínios da forma $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$. A demonstração desse resultado pode ser encontrada em $(1, Teorema\ 1.4.5)$. Não a explicitaremos aqui pelo fato dessa ser análoga à demonstração do resultado anterior.

Teorema 7. *Seja $m \equiv 1 \pmod 4$ um inteiro que não é quadrado perfeito tal que $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ seja um domínio de ideais principais. Seja p um primo ímpar tal que $\left(\frac{m}{p}\right) = 1$. Então existem inteiros u e v tais que:*

- $p = u^2+uv+\left(\frac{1-m}{4}\right)v^2$, *caso $m < 0$ ou $m > 0$ e existam inteiros T e U tais que $T^2+TU+\left(\frac{1-m}{4}\right)U^2 = -1$.*
- $p = u^2+uv+\left(\frac{1-m}{4}\right)v^2$ *ou* $p = -\left(u^2+uv+\left(\frac{1-m}{4}\right)v^2\right)$, *caso $m > 0$ e não existam inteiros T e U tais que $T^2+TU+\left(\frac{1-m}{4}\right)U^2 = -1$.*

Demonstração. Análoga à demonstração para $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. □

Tais resultados nos dão ferramentas importantes para o estudo de certas equações diofantinas para os valores de n e m inteiros livres de quadrados em que $\mathbb{Z}+\mathbb{Z}\sqrt{n}$ e $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ são domínios de ideais principais. Isso nos leva a questionar sobre quais valores de n e m tornam esses domínios de integridade em domínios de ideais principais. Responderemos parcialmente a esta questão ao longo dos próximos capítulos.

Prosseguimos agora analisando as relações entre elementos irredutíveis e primos, e os ideais de domínios de integridade e de ideias principais. Para este estudo, definiremos o conceito de ideal maximal.

Definição 13 (Ideal Maximal)**.** *Um ideal M de um domínio de integridade D é dito maximal se para todo I ideal de D que satisfaça $M \subset I \subset D$ tenha-se $I = M$ ou $I = D$.*

Apresentemos uma relação entre ideais maximais principais de um domínio de integridade e elementos irredutíveis desse domínio.

Teorema 8. *Sejam D um domínio de integridade, $a \in D$ tal que $a \neq 0$ e $a \notin U(D)$. Se $\langle a\rangle$ é um ideal maximal de D, então a é irredutível em D.*

Demonstração. Suponha que a não é um elemento irredutível de D. Então existem $b, c \in D \setminus U(D)$ tais que $a = bc$ e $b, c \neq 0$. Assim, $\langle a\rangle \subset \langle b\rangle \subset D$ (pela Proposição 3). Ainda, pelo Teorema 2, temos $c = \frac{a}{b} \notin U(D) \Rightarrow \langle a\rangle \neq \langle b\rangle$ e $b \notin U(D) \Rightarrow \langle b\rangle \neq \langle 1\rangle = D$, o que contraria a maximalidade de $\langle a\rangle$. □

O próximo exemplo mostra que a recíproca do Teorema 8 nem sempre é verdade:

Exemplo 4. *x é um elemento irredutível de $\mathbb{Z}[x]$ mas $\langle x\rangle$ não é ideal maximal de $\mathbb{Z}[x]$, pois $\langle x\rangle \subsetneq \langle 2, x\rangle \subsetneq \mathbb{Z}[x]$.*

A recíproca do Teorema 8, entretanto, vale para domínios de ideais principais.

Teorema 9. *Sejam D um domínio de ideais principais, $a \in D$ tal que $a \neq 0$ e $a \notin U(D)$. Então, $\langle a\rangle$ é um ideal maximal de D se, e somente se, a é irredutível em D.*

Demonstração. O Teorema 8 mostra a ida. Assim, precisamos apenas mostrar a recíproca. Suponha que a é irredutível em D e $\langle a\rangle \subset D$ não é ideal maximal. Então existe um ideal I tal que $\langle a\rangle \subsetneq I \subsetneq D$. Como D é um domínio de ideais principais, existe $b \in D$ tal que $I = \langle b\rangle$. Assim: $\langle a\rangle \subsetneq \langle b\rangle \subsetneq D$, donde $b|a$ pela Proposição 3. Logo, existe $c \in D$ tal que $a = bc$. Como $\langle a\rangle \neq \langle b\rangle$, pelo Teorema 2 segue que $c = \frac{a}{b} \notin U(D)$. Ainda, $\langle b\rangle \neq \langle 1\rangle = D \Rightarrow b \notin U(D)$ (pelo mesmo teorema), o que contradiz a ser irredutível. Logo, devemos ter $\langle a\rangle$ maximal. □

Em particular, este teorema e o exemplo anterior implicam que $\mathbb{Z}[x]$ não é um domínio de ideais principais.

Mostremos agora uma relação entre um ideal I ser maximal e o quociente D/I.

Teorema 10. *Sejam D um domínio de integridade e I um ideal de D. Então, D/I é um corpo se e somente se I é um ideal maximal.*

Demonstração. ($\Rightarrow$) Suponha que D/I seja um corpo e seja J um ideal de D tal que $I \subsetneq J \subset D$. Então, existe $b \in J \setminus I$, donde $\overline{b} \in D/I$ com $\overline{b} \neq 0$. Como D/I é um corpo, existe $\overline{c} \in D/I$ tal que $\overline{b}\overline{c} = \overline{1}$. Assim: $\overline{bc} = \overline{1}$, donde $bc - 1 \in I \subset J$. Como $b \in J$ e $c \in D$, temos $bc \in J$. Daí, $bc - (bc - 1) = 1 \in J \Rightarrow J = D$.

($\Leftarrow$) Suponha que I seja maximal. Para mostrar que D/I é um corpo, basta mostrarmos que todo elemento $\overline{b} \in D/I$, com $\overline{b} \neq \overline{0}$, possui um inverso multiplicativo em D/I, uma vez que as outras propriedades seguem pela definição de D/I. Assim, seja $\overline{b}$ um elemento dessa forma. Considere:

$$B = \{x \in D \mid x = by + w, y \in D, w \in I\}$$

Como $0 \in D$, temos que $w \in I \Rightarrow w + b * 0 = w \in B$, donde $I \subset B$. Ainda, $m, n \in B \Rightarrow m = by + w, n = bz + u, y, z \in D$ e $w, u \in I \Rightarrow m + n = b(y + z) + (w + u)$, com $y + z \in D$ e $w + u \in I$ (pois I é ideal) $\Rightarrow m + n \in B$. Por fim, $m \in B, \alpha \in D \Rightarrow m = by + w, y \in D, w \in I \Rightarrow \alpha m = b(\alpha y) + \alpha w, \alpha y \in D$ e $\alpha w \in I$ (pois I é ideal) $\Rightarrow \alpha m \in B$. Logo, B é ideal de D. Assim, como I é maximal, devemos ter $B = I$ ou $B = D$. Mas $b \in B$ e $b \notin I$, donde $B = D$. Logo, $1 \in B \Rightarrow \exists\ y \in D$ e $w \in I$ com $1 = by + w \Rightarrow 1 - by = w \in I \Rightarrow \overline{1 - by} = \overline{0} \Rightarrow \overline{b}\overline{y} = \overline{1}$. Assim, $\exists\ \overline{y} = \overline{b}^{-1} \in D/I$. Portanto, D/I é um corpo. □

Mostramos, no Teorema 8, que o conceito de ideal maximal está, de certa forma, relacionado com o conceito de elemento irredutível em um domínio de integridade D. Entretanto, vimos que os elementos irredutíveis em D e os elementos primos desse domínio nem sempre coincidem. Isso nos leva a questionar se existe um tipo de ideal de D que esteja relacionado com os elementos primos de D. Nesse sentido, temos a seguinte definição:

Definição 14 (Ideal Primo)**.** *Um ideal P de um domínio de integridade D, com $P \neq D$ é dito um ideal primo se:*

$$a, b \in D \text{ e } ab \in P \Rightarrow a \in P \text{ ou } b \in P.$$

Mostremos, para ideais primos, resultados análogos aos provados para maximais.

Teorema 11. *Sejam D um domínio de integridade e $a \in D \setminus U(D), a \neq 0$. Então:*

$$\langle a \rangle \text{ é ideal primo de } D \Leftrightarrow a \text{ é primo em } D.$$

Demonstração. ($\Rightarrow$) Suponha que $\langle a\rangle$ é um ideal primo de D. Sejam $b, c \in D$ tais que $a = bc$. Então $bc \in \langle a\rangle \Rightarrow b \in \langle a\rangle$ ou $c \in \langle a\rangle \Rightarrow a \mid b$ ou $a \mid c$ (pela Proposição 3). Logo, a é primo em D.

($\Leftarrow$) Sejam a primo em D e $b, c \in D$ tais que $bc \in \langle a\rangle$. Então existe $k \in D$ tal que $ak = bc$. Assim, $a \mid bc$ e, sendo a primo, temos que $a \mid b$ ou $a \mid c \Rightarrow b \in \langle a\rangle$ ou $c \in \langle a\rangle$ (pela Proposição 3). Logo, $\langle a\rangle$ é um ideal primo de D. □

Teorema 12. *Sejam D um domínio de integridade e I um ideal de D. Então, D/I é um domínio de integridade se, e somente se, I é primo.*

Demonstração. ($\Rightarrow$) Suponha que D/I é um domínio de integridade e sejam $a, b \in D$ tais que $ab \in I$. Então $\overline{ab} = \overline{a}\overline{b} = \overline{0}$. Mas D/I é um domínio de integridade, donde devemos ter $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0} \Rightarrow a \in I$ ou $b \in I$. Assim, I é primo.

($\Leftarrow$) Seja I um ideal primo de D. Como I é um ideal próprio de D, D/I é um anel comutativo com unidade $\overline{1}$. Assim, para que D/I seja um domínio de integridade, é necessário mostrar apenas que D/I não possui divisores de zero. Sejam $a, b \in D$ com $\overline{a}\overline{b} = \overline{0}$. Então $\overline{ab} = \overline{0} \Rightarrow ab \in I \Rightarrow a \in I$ ou $b \in I$ (pois I é primo) $\Rightarrow \overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. Portanto, D/I não possui divisores de zero, donde é um domínio de integridade. □

Usando os resultados mostrados para ideais maximais, ideais primos e domínios de ideais principais, podemos mostrar os seguintes teoremas:

Teorema 13. *Sejam D um domínio de integridade e I um ideal maximal de D. Então I é um ideal primo de D.*

Demonstração. Seja I um ideal maximal de D. Então, pelo Teorema 10, temos que D/I é um corpo. Em particular, D/I é um domínio de integridade, donde, pelo teorema anterior, segue que I é primo. □

Teorema 14. *Sejam D um domínio de ideais principais e I um ideal próprio de D. Então:*

$$I \text{ é maximal} \Leftrightarrow I \text{ é primo.}$$

Demonstração. Pelo teorema anterior, já sabemos que a ida é válida. Nos resta mostrar a volta. Suponha que I é um ideal primo de D que não é maximal. Então existe um ideal J de D tal que:

$$I \subsetneq J \subsetneq D.$$

Como D é um domínio de ideais principais, existem $a, b \in D$ tais que $I = \langle a\rangle$ e $J = \langle b\rangle$. Como $\langle a\rangle \subset \langle b\rangle$, temos pela Proposição 3 que $b \mid a \Rightarrow a = bc$ para algum $c \in D$. Como $bc = a \in \langle a\rangle = I$ e I é primo, devemos ter $b \in I$ ou $c \in I$. Mas $b \in I \Rightarrow J = \langle b\rangle \subset I \subsetneq J$, o que é um absurdo. Logo, $c \in I = \langle a\rangle \Rightarrow a \mid c \Rightarrow c = ad$ para algum $d \in D \Rightarrow a = bc = abd$

e $a \neq 0 \Rightarrow bd = 1 \Rightarrow b \in U(D) \Rightarrow J = D$, o que contradiz $J \subsetneq D$. Logo, I ideal primo próprio de $D \Rightarrow I$ é maximal. □

Por fim, mostremos mais duas propriedades dos ideais primos.

Teorema 15. *Seja P um ideal próprio de um domínio de integridade D. Então P é um ideal primo se, e somente se, para quaisquer dois ideais A e B de D satisfazendo $AB \subset P$, tivermos que $A \subset P$ ou $B \subset P$.*

Demonstração. ($\Leftarrow$) Suponha que P é um ideal próprio de D com a propriedade:

$$AB \subset P \Rightarrow A \subset P \text{ ou } B \subset P$$

para A, B ideais de D. Sejam $a, b \in D$ tais que $ab \in P$ e seja $k \in \langle a \rangle \langle b \rangle$. Então, existem $n \in \mathbb{N}$, $a_1, ..., a_n \in \langle a \rangle$ e $b_1, ..., b_n \in \langle b \rangle$ tais que:

$$k = a_1 b_1 + ... + a_n b_n$$

Dado $i \in \{1, ..., n\}$, como $a_i \in \langle a \rangle$ e $b_i \in \langle b \rangle$, existem $l_i, r_i \in D$ tais que:

$$a_i = a l_i \text{ e } b_i = b r_i$$

Assim:

$$k = a_1 b_1 + ... + a_n b_n = ab(l_1 r_1) + ... + ab(l_n r_n) = ab(l_1 r_1 + ... + l_n r_n) = abC$$

com $C = l_1 r_1 + ... + l_n r_n \in D$. Como P é ideal, $ab \in P$ e $C \in D$, temos $k \in P$. Portanto, $\langle a \rangle \langle b \rangle \subset P$, donde $\langle a \rangle \subset P$ ou $\langle b \rangle \subset P$. No primeiro caso, temos $a \in P$, e no segundo, temos $b \in P$. Ou seja:

$$ab \in P \text{ implica em } a \in P \text{ ou } b \in P$$

donde P é um ideal primo.

($\Rightarrow$) Sejam P um ideal primo de D e A, B ideais de D tais que:

$$AB \subset P$$

Suponha que $A \not\subset P$. Então, existe $a \in A$ tal que $a \notin P$. Seja $b \in B$. Temos que $ab \in AB \subset P$. Como P é um ideal primo, vale que $a \in P$ ou $b \in P$. Uma vez que $a \notin P$, segue que $b \in P$. Portanto, $B \subset P$.

Logo, vale que $A \subset P$ ou $B \subset P$. □

Teorema 16. *Sejam D e D_1 domínios de integridade satisfazendo $D \subset D_1$ e P um ideal primo de D_1 tal que $P \cap D \neq \{0\}, D$. Então $P \cap D$ é um ideal primo de D.*

Demonstração. Sejam $a, b \in D \subset D_1$ tais que $ab \in P \cap D$. Então $ab \in P$, com $a, b \in D_1$ e P ideal primo de D_1. Pela definição de ideal primo, segue que $a \in P$ ou $b \in P$. No primeiro caso, como $a \in D$, segue que $a \in P \cap D$. No segundo caso, como $b \in D$, segue que $b \in P \cap D$. Portanto:

$$a, b \in D \text{ e } ab \in P \cap D \text{ implica em } a \in P \cap D \text{ ou } b \in P \cap D$$

donde $P \cap D$ é um ideal primo de D. □

2.3 SOMA E PRODUTO DE IDEAIS

Estudaremos nesta seção a soma e o produto de ideais. Este conceito será usado ao estudarmos os domínios de Dedekind e a fatoração de ideais, os quais serão essenciais no estudo das equações diofantinas. Comecemos então com a soma de ideais.

Definição 15 (Soma de ideais)**.** *Sejam D um domínio de integridade e $I, J \subset D$ ideais de D. A soma de I e J, denotada por $I + J$, é o ideal de D:*

$$I + J = \{i + j \mid i \in I, j \in J\}$$

Da definição de $I + J$, vemos que $I + J \subset D$. Resta mostrarmos que $I + J$ é, de fato, um ideal de D.

- $0 \in I + J$: Como I, J são ideais, temos que $0 \in I, J$. Assim, $0 = 0 + 0 \in I + J$.
- $a, b \in I + J$ implica em $a + b \in I + J$: Como $a, b \in I + J$, existem $i_1, i_2 \in I$ e $j_1, j_2 \in J$ tais que:

  $$a = i_1 + j_1$$
  $$b = i_2 + j_2$$

  Como I e J são ideais, temos $i_1 + i_2 \in I$ e $j_1 + j_2 \in J$. Assim:

  $$a + b = i_1 + j_1 + i_2 + j_2 = (i_1 + i_2) + (j_1 + j_2) \in I + J$$

- $a \in I + J$ e $d \in D$ implica em $ad \in I + J$: Como $a \in I + J$, existem $i \in I$ e $j \in J$ tais que $i + j = a$. Como I e J são ideais, temos $id \in I$ e $jd \in J$. Assim:

  $$ad = (i + j)d = id + jd \in I + J$$

Logo, $I + J$ é ideal de D. Provaremos agora algumas propriedades da soma de ideais, cujas demonstrações são fornecidas pelo autor deste texto.

Proposição 5. *Sejam D um domínio de integridade e $I, J, K \subset D$ ideais de D. Então:*

1. $I + J = J + I$.
2. $I + (J + K) = (I + J) + K$.
3. $I + \langle 0 \rangle = I$.
4. $I + \langle 1 \rangle = \langle 1 \rangle$.
5. *Se existem* $i, j \in D$ *tais que* $I = \langle i \rangle$ *e* $J = \langle j \rangle$, *então* $I + J = \langle i, j \rangle$.
6. *Se* $K \subset D$ *é um ideal de* D *que satisfaz* $I, J \subset K$, *então* $I + J \subset K$.
7. $I, J \subset I + J$.

Demonstração. 1. Dado $x \in I + J$, existem $i \in I$ e $j \in J$ tais que:

$$x = i + j = j + i \in J + I$$

donde $I + J \subset J + I$. Por simetria, temos $J + I \subset I + J$. Assim, $I + J = J + I$.

2. Dado $x \in I + (J + K)$, existem $i \in I$, $j \in J$ e $k \in K$ tais que:

$$x = i + (j + k) = (i + j) + k \in (I + J) + K$$

donde $I + (J + K) \subset (I + J) + K$. Pelo item 1 e pelo que já mostramos, temos:

$$(I + J) + K = K + (J + I) \subset (K + J) + I = I + (J + K)$$

Logo, $I + (J + K) = (I + J) + K$.

3. Dado $x \in I + \langle 0 \rangle$, temos que existe $i \in I$ tal que $x = i + 0 = i \in I$. Por outro lado, dado $i \in I$, temos $i = i + 0 \in I + \langle 0 \rangle$. Logo, $I + \langle 0 \rangle = I$.

4. Dado $x \in D = \langle 1 \rangle$, temos que $x = 0 + x \in I + \langle 1 \rangle$ (uma vez que I é ideal e, portanto, $0 \in I$). Como $I + \langle 1 \rangle \subset D = \langle 1 \rangle$, temos $I + \langle 1 \rangle = \langle 1 \rangle$.

5. Seja $x \in I + J$. Então, existem $r, s \in D$ tais que $x = ri + sj \in \langle i, j \rangle$. Analogamente, dado $y \in \langle i, j \rangle$, existem $r, s \in D$ tais que $y = ir + js$. Como I e J são ideais, temos que $ir \in I$ e $js \in J$, donde $y \in I + J$. Com isso, segue que $I + J = \langle i, j \rangle$.

6. Seja $x \in I + J$. Então existem $i \in I \subset K$ e $j \in J \subset K$ tais que $x = i + j \in K$ (pois K é ideal). Logo, $I + J \subset K$.

7. Seja $i \in I$. Como $0 \in J$, temos $i = i + 0 \in I + J$, donde $I \subset I + J$. Analogamente, $J \subset I + J$.

□

Note que a penúltima condição da proposição anterior implica que $I + J$ é o menor ideal de D que contém I e J.

Prosseguimos agora com a definição de produto de ideais e com suas propriedades.

Definição 16 (Produto de ideais)**.** *Sejam I e J ideais de um domínio de integridade D. O produto de I e J, denotado por IJ, é o ideal de D definido por:*

$$IJ = \{x \in D \mid x = i_1j_1 + ... + i_rj_r \text{ para algum } r \in \mathbb{N}, \text{ com } i_1, ..., i_r \in I \text{ e } j_1, ..., j_r \in J\}$$

É evidente que $IJ \subset D$. Vamos mostrar que esse produto é de fato um ideal:

1. $0 \in IJ$: Como $0 \in I, J$, temos $0 = 0 \times 0 \in IJ$.

2. $a, b \in IJ \Rightarrow a+b \in IJ$: Se $a, b \in IJ$, existem $a_1, ..., a_r, c_1, ..., c_n \in I$ e $b_1, ..., b_r, d_1, ..., d_n \in J$ tais que:

$$a = a_1b_1 + ... + a_rb_r$$
$$b = c_1d_1 + ... + c_nd_n$$

   Fazendo $i_k = a_k, j_k = b_k$ para $k \in \{1, ..., r\}$ e $i_{k+r} = c_k, j_{k+r} = d_k$ para $k \in \{1, ..., n\}$, temos que $i_k \in I$ e $j_k \in J$ para todo $k \in \{1, ..., n + r\}$. Assim:

$$a + b = a_1b_1 + ... + a_rb_r + c_1d_1 + ... + c_nd_n = i_1j_1 + ... + i_{n+r}j_{n+r} \in IJ$$

3. $d \in D, a \in IJ \Rightarrow da \in IJ$: Como $a \in IJ$, existem $a_1, ..., a_r \in I$ e $b_1, ..., b_r \in J$ tais que:

$$a = a_1b_1 + ... + a_rb_r$$

   Como $a_k \in I(ideal)$ para $k \in \{1, ..., r\}$ e $d \in D$, temos $da_k = A_k \in I$ para $k \in \{1, ..., r\}$. Portanto:

$$da = d(a_1b_1 + ... + a_rb_r) = (da_1)b_1 + ... + (da_r)b_r = A_1b_1 + ... + A_rb_r \in IJ$$

   Portanto, IJ é de fato um ideal de D.

   As demonstrações da proposição a seguir são fornecidas pelo autor deste texto.

Proposição 6. *Sejam D um domínio de integridade, $I, J, K \subset D$ ideais de D. Então:*

1. $IJ = JI$.

2. $I(JK) = (IJ)K$.

3. $I\langle 0\rangle = \langle 0\rangle$.

4. $I\langle 1\rangle = I$.

5. *Se existem* $i, j \in D$ *tais que* $I = \langle i \rangle$ *e* $J = \langle j \rangle$*, então* $IJ = \langle ij \rangle$.

6. $(I + J)\,K = IK + JK$.

7. $IJ \subset I$ *e* $IJ \subset J$.

Demonstração. 1. Seja $x \in IJ$. Então, existem $i_1, ..., i_n \in I$ e $j_1, ..., j_n \in J$ tais que:

$$x = i_1 j_1 + ... + i_n j_n = j_1 i_1 + ... + j_n i_n \in JI$$

Assim, $IJ \subset JI$. Pela simetria, temos $JI \subset IJ$, donde segue que $IJ = JI$.

2. Seja $x \in I(JK)$. Então, existem $i_1, ..., i_n \in I$ e $y_1, ..., y_n \in JK$ tais que:

$$x = i_1 y_1 + ... + i_n y_n$$

Dado $k \in \{1, ..., n\}$, como $y_k \in JK$, existem $j_{k,1}, ..., j_{k,m_k} \in J$ e $u_{k,1}, ..., u_{k,m_k} \in K$ tais que:

$$y_k = j_{k,1} u_{k,1} + ... + j_{k,m_k} u_{k,m_k}$$

Assim:

$$x = i_1(j_{1,1} u_{1,1} + ... + j_{1,m_1} u_{1,m_1}) + ... + i_n(j_{n,1} u_{n,1} + ... + j_{n,m_n} u_{n,m_n}) =$$
$$= i_1 j_{1,1} u_{1,1} + ... + i_1 j_{1,m_1} u_{1,m_1} + ... + i_n j_{n,1} u_{n,1} + ... + i_n j_{n,m_n} u_{n,m_n}$$

Dados $k \in \{1, ..., n\}$ e $l \in \{1, ..., m_k\}$, seja $z_{k,l} = i_k j_{k,l} \in IJ$. Então:

$$x = z_{1,1} u_{1,1} + ... + z_{1,m_1} u_{1,m_1} + ... + z_{n,1} u_{n,1} + ... + z_{n,m_n} u_{n,m_n} \in (IJ)K$$

Logo, $I(JK) \subset (IJ)K$. Ainda, pelo item 1 e pelo que mostramos, temos:

$$(IJ)K = K(JI) \subset (KJ)I = I(JK)$$

Portanto, $I(JK) = (IJ)K$.

3. Seja $x \in I\,\langle 0 \rangle$. Então existem $i_1, ..., i_n \in I$ tais que:

$$x = i_1 0 + ... + i_n 0 = 0 + ... + 0 = 0 \in \langle 0 \rangle$$

Ainda, como $0 \in I\,\langle 0 \rangle$ (pois $I\,\langle 0 \rangle$ é ideal), temos $I\,\langle 0 \rangle = \langle 0 \rangle$.

4. Seja $x \in I\,\langle 1 \rangle$. Então, existem $i_1, ..., i_n \in I$ e $y_1, ..., y_n \in \langle 1 \rangle = D$ tais que:

$$x = i_1 y_1 + ... + i_n y_n \in I$$

pois $i_j y_j \in I$ para todo $j \in \{1, ..., n\}$ (pois I é ideal). Ainda, $i \in I$ é tal que:

$$i = i \times 1 \in I\,\langle 1 \rangle$$

Logo, $I\,\langle 1 \rangle = I$.

5. Seja $x \in IJ$. Então existem $r_1, ..., r_n, s_1, ..., s_n \in D$ tais que:

$$x = ir_1js_1 + ... + ir_njs_n = ij(r_1s_1 + ... + r_ns_n) \in \langle ij \rangle$$

Analogamente, seja $y \in \langle ij \rangle$. Então, existem $u_1, ..., u_n \in D$ tais que:

$$y = iju_1 + ... + iju_n = (i \times 1)(ju_1) + ... + (i \times 1)(ju_n) \in IJ$$

Logo, $IJ = \langle ij \rangle$.

6. Seja $x \in (I + J)K$. Então existem $i_1, ..., i_n \in I$, $j_1, ..., j_n \in J$ e $k_1, ..., k_n \in K$ tais que:

$$x = (i_1 + j_1)k_1 + ... + (i_n + j_n)k_n = (i_1k_1 + ... + i_nk_n) + (j_1k_1 + ... + j_nk_n) \in IK + JK$$

Por outro lado, seja $y \in IK + JK$. Então existem $i_1, ..., i_n \in I \subset I + J$, $j_1, ..., j_m \in J \subset I + J$ e $k_1, ..., k_n, k'_1, ..., k'_m \in K$ tais que:

$$y = i_1k_1 + ... + i_nk_n + j_1k'_1 + ... + j_mk'_m \in (I + J)K$$

Portanto, $(I + J)K = IK + JK$.

7. Seja $x \in IJ$. Então existem $i_1, ..., i_n \in I$ e $j_1, ..., j_n \in J$ tais que:

$$x = i_1j_1 + ... + i_nj_n$$

Como I é ideal, $i_k \in I$ e $j_k \in D$ para $k \in \{1, ..., n\}$ temos $i_kj_k \in I$ para $k \in \{1, ..., n\}$, donde $x \in I$. Assim, $IJ \subset I$. Analogamente, $IJ \subset J$.

□

2.4 DOMÍNIOS EUCLIDIANOS

No estudo da Teoria dos Números, muitos resultados importantes são derivados do algoritmo da divisão de Euclides. Estudaremos agora domínios Euclidianos, que são domínios que possuem uma propriedade similar à do algoritmo da divisão. Veremos que domínios com esta propriedade satisfazem muitos resultados importantes, como a de serem, em particular, domínios de ideais principais. Para isso, começaremos definindo uma função euclidiana e estudando suas propriedades.

Definição 17 (Função euclidiana)**.** *Seja D um domínio de integridade. Uma função $\phi : D \to \mathbb{Z}$ é dita uma função euclidiana em D se ela satisfaz as seguintes propriedades:*

- $\phi(ab) \geq \phi(a), \forall\ a, b \in D$ *com* $b \neq 0$.
- *Se* $a, b \in D$ *com* $b \neq 0$ *então existem* $q, r \in D$ *tais que* $a = qb + r$ *e* $\phi(r) < \phi(b)$.

Teorema 17 (Propriedades de uma função euclidiana)**.** *Sejam D um domínio de integridade que possui uma função euclidiana ϕ e $a, b \in D$. Então:*

1. $a \sim b \Rightarrow \phi(a) = \phi(b)$.
2. $\phi(a) > \phi(0)$ *se* $a \neq 0$.
3. $a \mid b$ *e* $\phi(a) = \phi(b) \Rightarrow a \sim b$.
4. $a \in U(D) \Leftrightarrow \phi(a) = \phi(1)$.

Demonstração. 1. Primeiramente, notemos que $a \sim 0 \Rightarrow a = 0$. De fato, como $0 \times b = 0$ para todo $b \in D$, temos que $0 \mid a \Rightarrow a = 0$. Assim, $a \sim 0 \Rightarrow 0 \mid a \Rightarrow a = 0 \Rightarrow \phi(a) = \phi(0)$. Logo, se $a = 0$ ou $b = 0$, a implicação vale. Se $a \sim b$ e $a, b \neq 0$, então existem $u, v \in D \setminus \{0\}$ tais que $b = au$ e $a = bv$. Pela primeira propriedade de funções euclidianas, temos: $\phi(a) = \phi(bv) \geq \phi(b) = \phi(au) \geq \phi(a)$, donde $\phi(a) = \phi(b)$.

2. Sendo $a \neq 0$, pela segunda propriedade de função euclidiana, temos que existem $q, r \in D$ tais que $0 = aq + r$, com $\phi(r) < \phi(a)$. Suponha que $r \neq 0$. Então $q \neq 0$ e pela primeira propriedade, temos $\phi(r) = \phi((-q)a) \geq \phi(a)$, o que é uma contradição. Logo, $r = 0$ e, assim, $\phi(a) > \phi(0)$.

3. Se $b = 0$, temos que $\phi(a) = \phi(b) = \phi(0) \Rightarrow a = 0 = b \Rightarrow a \sim b$, pelo item anterior. Se $b \neq 0$, pela segunda propriedade de funções euclidianas, existem $q, r \in D$ tais que $a = qb + r$ e $\phi(r) < \phi(b) = \phi(a)$. Suponha que $r \neq 0$. Como $a \mid b$, existe $u \in D$ tal que $b = au$. Assim, $r = a - bq = a - auq = a(1 - uq) \neq 0$, donde $a \neq 0$ e $1 - uq \neq 0$. Pela primeira propriedade de funções euclidianas, temos $\phi(r) = \phi(a(1 - uq)) \geq \phi(a)$, o que é um absurdo pois $\phi(r) < \phi(a)$. Portanto, $r = 0$ e $a = qb \Rightarrow b \mid a$. Como $a \mid b$, segue que $a \sim b$.

4. Se $a \in U(D)$, temos $a \sim 1 \Rightarrow \phi(a) = \phi(1)$ pelo item 1. Por outro lado, se $\phi(a) = \phi(1)$, como $1 \mid a$ (pois 1 divide todos os elementos de D), temos pelo item 3 que $a \sim 1 \Rightarrow a \in U(D)$.

□

Vejamos agora a definição de um domínio Euclidiano, e mostremos que todo domínio Euclidiano é, também, um domínio de ideais principais.

Definição 18 (Domínio Euclidiano)**.** *Seja D um domínio de integridade. Se D possui uma função euclidiana ϕ então D é chamado de domínio Euclidiano com respeito a ϕ.*

Teorema 18. *Um domínio Euclidiano é um domínio de ideais principais.*

Demonstração. Seja D um domínio Euclidiano. Então D possui uma função euclidiana ϕ. Seja I um ideal de D. Se $I = \{0\}$, então $I = \langle 0 \rangle$ é um ideal principal. Se $I \neq \{0\}$, seja $S \subset \mathbb{Z}$ dado por:

$$S = \{\phi(x) | x \in I, x \neq 0\}$$

Como $I \neq \{0\}$, temos $S \neq \emptyset$. Ainda, pelo item 2 do Teorema 17, temos $\phi(x) > \phi(0)\ \forall\ x \in I, x \neq 0$. Logo, S é limitado inferiormente por $\phi(0)$. Pelo PBO, S possui um menor elemento y. Pela definição de S, existe $a \in I, a \neq 0$ tal que $y = \phi(a)$. Como $a \in I$ (ideal), temos $\langle a \rangle \subset I$. Suponha que $I \neq \langle a \rangle$. Então existe $b \in I \setminus \langle a \rangle$. Em particular, como $0 \in \langle a \rangle$, temos $b \neq 0$. Pela segunda propriedade das funções euclidianas, existem $q, r \in D$ tais que $b = aq + r$, com $\phi(r) < \phi(a)$. Assim, $r = b - aq$ e, como I é ideal, $a, b \in I$ e $q \in D$, temos $r \in I$. Ainda, $r = 0 \Rightarrow b = aq \Rightarrow b \in \langle a \rangle$, o que é falso, por isso $r \neq 0$. Logo, $\phi(r) \in S \Rightarrow \phi(r) \geq \min S = \phi(a) > \phi(r)$ (absurdo). Portanto, $I = \langle a \rangle$, donde I é um ideal principal. Assim, todo ideal de D é principal, donde D é um domínio de ideais principais. □

Mostraremos agora que os domínios Euclidianos satisfazem um resultado análogo ao do algoritmo de Euclides para os números inteiros.

Teorema 19 (Algoritmo de Euclides)**.** *Sejam D um domínio Euclidiano em relação a ϕ e $a, b \in D \setminus \{0\}$. Definamos recursivamente as sequências $q_1, q_2, ...$ e $r_{-1}, r_0, r_1, ...$ de elementos de D pelas relações:*

$$r_{-1} = a, r_0 = b,\ \text{e } r_j = q_{j+2} r_{j+1} + r_{j+2} \text{ com } \phi(r_{j+2}) < \phi(r_{j+1})$$

Com $j = -1, 0, 1, ..., k$, sendo $k \geq -1$ o menor tal que $r_{k+2} = 0$. Então, $\langle a, b \rangle = \langle r_{k+1} \rangle$.

Demonstração. Pela propriedade 2 da função euclidiana ϕ, o processo de construção das sequências (r_j) e (q_l) está bem definido para $j = -1, 0, 1, ..., k+2$ e $l = 1, 2, ..., k+2$. Ainda, $\phi(r_1) > \phi(r_2) > \phi(r_3) > ...$ é uma sequência decrescente limitada inferiormente por $\phi(0)$ (pelo item 2 do Teorema 17), donde existe $k + 2 \in \mathbb{N}$ tal que $\phi(r_j) > \phi(0)$ se $j < k + 2$ e $\phi(r_{k+2}) = \phi(0) \Rightarrow r_{k+2} = 0$ (pelo item 2 do Teorema 17). Assim, dado $j \in \{-1, 0, 1, 2, ..., k\}$ e usando a definição dos r_j, temos:

$$\langle r_j, r_{j+1} \rangle = \langle q_{j+2} r_{j+1} + r_{j+2}, r_{j+1} \rangle = \langle r_{j+2}, r_{j+1} \rangle = \langle r_{j+1}, r_{j+2} \rangle$$

Portanto:

$$\langle a, b \rangle = \langle r_{-1}, r_0 \rangle = \langle r_0, r_1 \rangle = ... = \langle r_k, r_{k+1} \rangle = \langle r_{k+1}, r_{k+2} \rangle = \langle r_{k+1}, 0 \rangle = \langle r_{k+1} \rangle$$

□

Note que, na definição de domínios Euclidianos, necessitamos de uma função euclidiana, a qual não sabemos se existe para um dado domínio e, caso exista, não sabemos

como encontrá-la. Estudaremos então uma classe de funções que aparecem naturalmente como candidatas à funções euclidianas para certos domínios de integridade, devido às suas propriedades. Conseguiremos então provar critérios necessários e suficientes para que $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ e $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ sejam Euclidianos com relações a essas funções.

Definição 19 (Função ϕ_m)**.** *Seja $m \in \mathbb{Z}$ livre de quadrados. A função $\phi_m : \mathbb{Q}(\sqrt{m}) \longrightarrow \mathbb{Q}$ é dada por:*

$$\phi_m(r+s\sqrt{m}) = \left|r^2 - ms^2\right|$$

Para todos $r, s \in \mathbb{Q}$.

Lema 1 (Propriedades da ϕ_m)**.** *Seja $m \in \mathbb{Z}$ livre de quadrados. Então:*

1. *$\phi_m : \mathbb{Z}+\mathbb{Z}\sqrt{m} \longrightarrow \mathbb{N}\cup\{0\}$, isto é, se $\alpha \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$, então $\phi_m(\alpha) \in \mathbb{N}\cup\{0\}$.*
2. *Se $m \equiv 1 \pmod 4$ então $\phi_m : \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \longrightarrow \mathbb{N}\cup\{0\}$, isto é, se $\alpha \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, então $\phi_m(\alpha) \in \mathbb{N}\cup\{0\}$.*
3. *Seja $\alpha \in \mathbb{Q}(\sqrt{m})$. Então $\phi_m(\alpha) = 0 \Leftrightarrow \alpha = 0$.*
4. *$\phi_m(\alpha\beta) = \phi_m(\alpha)\phi_m(\beta)$ para todo $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$.*
5. *$\phi_m(\alpha\beta) \geq \phi_m(\alpha)$ para todo $\alpha, \beta \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$ com $\beta \neq 0$.*
6. *Se $m \equiv 1 \pmod 4$, então $\phi_m(\alpha\beta) \geq \phi_m(\alpha)$ para todo $\alpha, \beta \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ com $\beta \neq 0$.*

Demonstração.

1. Seja $\alpha \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$. Então $\alpha = x+y\sqrt{m}$, com $x, y \in \mathbb{Z} \Rightarrow x^2 - my^2 \in \mathbb{Z} \Rightarrow |x^2 - my^2| = \phi_m(\alpha) \in \mathbb{N}\cup\{0\}$.

2. Se $m \equiv 1 \pmod 4$, então $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ é um domínio de integridade. Seja $\alpha \in \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, de forma que $\alpha = x+y\left(\frac{1+\sqrt{m}}{2}\right) = \left(x+\frac{y}{2}\right)+\frac{y}{2}\sqrt{m}$, com $x, y \in \mathbb{Z}$. Então:

$$\begin{aligned}\phi_m(\alpha) = \phi_m\left(\left(x+\frac{y}{2}\right)+\frac{y}{2}\sqrt{m}\right) &= \left|\left(x+\frac{y}{2}\right)^2 - m\left(\frac{y}{2}\right)^2\right| \\ &= \left|x^2+xy+\frac{(1-m)}{4}y^2\right| \in \mathbb{N}\cup\{0\}\end{aligned}$$

Pois $\frac{1-m}{4} \in \mathbb{Z}$, uma vez que $m \equiv 1 \pmod 4$.

3. Seja $\alpha \in \mathbb{Q}(\sqrt{m})$, de forma que $\alpha = r + s\sqrt{m}$, com $r, s \in \mathbb{Q}$. Então, como m é livre de quadrados, temos:

$$\begin{aligned}\phi_m(\alpha) = 0 &\Leftrightarrow \phi_m(r + s\sqrt{m}) = 0\\ &\Leftrightarrow \left|r^2 - ms^2\right| = 0\\ &\Leftrightarrow r^2 = ms^2\\ &\Leftrightarrow r = \pm s\sqrt{m}\\ &\Leftrightarrow r = s = 0\\ &\Leftrightarrow r + s\sqrt{m} = 0\\ &\Leftrightarrow \alpha = 0\end{aligned}$$

   Pois $r \in \mathbb{Q}$ e $s\sqrt{m} \in \mathbb{R} \setminus \mathbb{Q}$ (já que $m \in \mathbb{Z}$ é livre de quadrados).

4. Sejam $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$. Então $\alpha = x + y\sqrt{m}$ e $\beta = r + s\sqrt{m}$ com $x, y, r, s \in \mathbb{Q}$. Assim:

$$\begin{aligned}\phi_m(\alpha\beta) &= \phi_m((x + y\sqrt{m})(r + s\sqrt{m})) = \phi_m((xr + mys) + (xs + yr)\sqrt{m})\\ &= \left|(xr + mys)^2 - m(xs + yr)^2\right|\\ &= \left|x^2r^2 + 2xrmys + m^2y^2s^2 - mx^2s^2 - 2xrmys - my^2r^2\right|\\ &= \left|x^2r^2 + m^2y^2s^2 - mx^2s^2 - my^2r^2\right|\\ &= \left|(x^2 - my^2)(r^2 - ms^2)\right| = \left|x^2 - my^2\right|\left|r^2 - ms^2\right|\\ &= \phi_m(x + y\sqrt{m})\phi_m(r + s\sqrt{m})\\ &= \phi_m(\alpha)\phi_m(\beta)\end{aligned}$$

5. Sejam $\alpha, \beta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, com $\beta \neq 0$. Pelo item 3, temos $\phi_m(\beta) \neq 0$. Pelo item 1, $\phi_m(\alpha), \phi_m(\beta) \in \mathbb{N} \cup \{0\} \Rightarrow \phi_m(\alpha) \geq 0$ e $\phi_m(\beta) \geq 1$. Por fim, pelo item 4:

$$\phi_m(\alpha\beta) = \phi_m(\alpha)\phi_m(\beta) \geq \phi_m(\alpha)$$

6. Sejam $\alpha, \beta \in \mathbb{Z} + \mathbb{Z}\left(\dfrac{1 + \sqrt{m}}{2}\right)$, com $\beta \neq 0$. Pelo item 3, temos $\phi_m(\beta) \neq 0$. Pelo item 2, $\phi_m(\alpha), \phi_m(\beta) \in \mathbb{N} \cup \{0\} \Rightarrow \phi_m(\alpha) \geq 0$ e $\phi_m(\beta) \geq 1$. Por fim, pelo item 4:

$$\phi_m(\alpha\beta) = \phi_m(\alpha)\phi_m(\beta) \geq \phi_m(\alpha)$$

□

Usando as propriedades da função ϕ_m, podemos chegar a um critério necessário e suficiente para que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ seja Euclidiano com relação a ϕ_m.

Teorema 20. *Seja $m \in \mathbb{Z}$ livre de quadrados. Então, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com relação a ϕ_m se, e somente se, para todos $x, y \in \mathbb{Q}$ existem $a, b \in \mathbb{Z}$ tais que:*

$$\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) < 1 \tag{2.2}$$

Demonstração. ($\Rightarrow$) Suponha que $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ seja euclidiano com respeito a ϕ_m. Sejam $x, y \in \mathbb{Q}$. Então existem $r, s, t \in \mathbb{Z}$, com $t \neq 0$, tais que $x = \dfrac{r}{t}$ e $y = \dfrac{s}{t}$, de forma que $x + y\sqrt{m} = \dfrac{r + s\sqrt{m}}{t}$. Como ϕ_m é função euclidiana em $\mathbb{Z}+\mathbb{Z}\sqrt{m}$, existem $a+b\sqrt{m}, c+d\sqrt{m} \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$ tais que:

$$r + s\sqrt{m} = t(a + b\sqrt{m}) + (c + d\sqrt{m}), \phi_m(c + d\sqrt{m}) < \phi_m(t)$$

Então:

$$\begin{aligned}
\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) &= \phi_m\left(\frac{r + s\sqrt{m}}{t} - (a + b\sqrt{m})\right) \\
&= \phi_m\left(\frac{r + s\sqrt{m} - (a + b\sqrt{m})t}{t}\right) \\
&= \phi_m\left(\frac{c + d\sqrt{m}}{t}\right) \\
&= \frac{\phi_m(c + d\sqrt{m})}{\phi_m(t)} < 1
\end{aligned}$$

Pelo item 4 do Lema 1.

($\Leftarrow$) Suponha que (2.2) valha. Já sabemos que $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ é domínio de integridade. Assim, para mostrar que $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ é domínio Euclidiano, devemos verificar que ϕ_m satisfaz as propriedades de uma função euclidiana em $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. Pelo item 5 do Lema 1, a primeira propriedade já é válida. Para mostrar a segunda propriedade, sejam $r + s\sqrt{m}, t + u\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, com $t + u\sqrt{m} \neq 0$. Então $t \neq 0$ ou $u \neq 0$, e portanto:

$$\begin{aligned}
\frac{r + s\sqrt{m}}{t + u\sqrt{m}} = \frac{(r + s\sqrt{m})(t - u\sqrt{m})}{(t + u\sqrt{m})(t - u\sqrt{m})} &= \frac{(rt - usm) + (st - ru)\sqrt{m}}{t^2 - mu^2} \\
&= \frac{rt - usm}{t^2 - mu^2} + \frac{(st - ru)}{t^2 - mu^2}\sqrt{m}
\end{aligned}$$

Assim, tomando $x = \dfrac{rt - usm}{t^2 - mu^2}, y = \dfrac{(st - ru)}{t^2 - mu^2} \in \mathbb{Q}$, temos:

$$x + y\sqrt{m} = \frac{rt - usm}{t^2 - mu^2} + \frac{st - ru}{t^2 - mu^2}\sqrt{m} = \frac{r + s\sqrt{m}}{t + u\sqrt{m}}$$

Por (2.2), existem $a, b \in \mathbb{Z}$ tais que:

$$\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) < 1$$

Sejam $c = r - at - bum, d = s - au - bt \in \mathbb{Z}$. Então:

$$\begin{aligned}
c + d\sqrt{m} &= (r - at - bum) + (s - au - bt)\sqrt{m} = (r + s\sqrt{m}) - ((at + bum) + (au + bt)\sqrt{m}) \\
&= (r + s\sqrt{m}) - (a + b\sqrt{m})(t + u\sqrt{m}) \in \mathbb{Z} + \mathbb{Z}\sqrt{m}
\end{aligned}$$

Assim, $r + s\sqrt{m} = (a + b\sqrt{m})(t + u\sqrt{m}) + (c + d\sqrt{m})$ e:

$$\begin{aligned}\phi_m(c + d\sqrt{m}) &= \phi_m((r + s\sqrt{m}) - (a + b\sqrt{m})(t + u\sqrt{m})) \\ &= \phi_m((x + y\sqrt{m})(t + u\sqrt{m}) - (a + b\sqrt{m})(t + u\sqrt{m})) \\ &= \phi_m(t + u\sqrt{m})\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) \\ &< \phi_m(t + u\sqrt{m})\end{aligned}$$

Utilizando o item 4 do Lema 1 e o fato de que $t + u\sqrt{m} \neq 0$ e $t + u\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m} \Rightarrow \phi_m(t + u\sqrt{m}) \geq 1$ (pelo item 1 do Lema 1). Portanto, ϕ_m é uma função euclidiana em $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ e, assim, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é domínio Euclidiano. □

Usando o teorema anterior, podemos determinar os inteiros livres de quadrados m negativos tais que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é domínio Euclidiano com relação a ϕ_m.

Proposição 7. *Seja $m \in \mathbb{Z}$ um inteiro negativo livre de quadrados. O domínio de integridade $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com respeito a ϕ_m se, e somente se, $m = -1, -2$.*

Demonstração. Primeiramente, mostraremos que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com respeito a ϕ_m para $m = -1, -2$. Sejam $x, y \in \mathbb{Q}$. Então, existem $a, b \in \mathbb{Z}$ tais que:

$$|x - a| \leq \frac{1}{2} \text{ e } |y - b| \leq \frac{1}{2}$$

Assim, se $m \in \{-1, -2\}$, temos $|m| \leq 2$, donde:

$$\begin{aligned}\phi_m((x + y\sqrt{m}) - (a + b\sqrt{m})) &= \phi_m((x - a) + (y - b)\sqrt{m}) \\ &= \left|(x - a)^2 - m(y - b)^2\right| \\ &\leq |x - a|^2 + |m|\,|y - b|^2 \\ &\leq \frac{1}{4} + \frac{|m|}{4} \\ &\leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1\end{aligned}$$

Pelo teorema anterior, segue que $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ é Euclidiano com relação a ϕ_m para $m = -1, -2$.

Por outro lado, suponha que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com respeito à ϕ_m. Então, pelo teorema anterior, existem $a, b \in \mathbb{Z}$ tais que:

$$\begin{aligned}\phi_m\left(\left(\frac{1}{2} + \frac{1}{2}\sqrt{m}\right) - (a + b\sqrt{m})\right) < 1 \\ \phi_m\left(\left(\frac{1}{2} - a\right) + \left(\frac{1}{2} - b\sqrt{m}\right)\right) < 1 \\ \left|\left(\frac{1}{2} - a\right)^2 - m\left(\frac{1}{2} - b\right)^2\right| < 1\end{aligned}$$

Como $m < 0$, temos $-m = |m| > 0$. Ainda, $\left|\frac{1}{2} - a\right|^2, \left|\frac{1}{2} - b\right|^2 \geq 0$, donde:

$$\left|\left(\frac{1}{2} - a\right)^2 - m\left(\frac{1}{2} - b\right)^2\right| = \left(\frac{1}{2} - a\right)^2 - m\left(\frac{1}{2} - b\right)^2 < 1$$

Sabemos ainda que, como $a, b \in \mathbb{Z}$, temos $\left(\frac{1}{2} - a\right) \geq \frac{1}{2}$ e $\left(\frac{1}{2} - b\right) \geq \frac{1}{2}$. Assim:

$$\frac{1}{4} - \frac{m}{4} \leq \left(\frac{1}{2} - a\right)^2 - m\left(\frac{1}{2} - b\right)^2 < 1$$
$$1 - m < 4$$
$$m > -3$$

Portanto, $m = -1$ e $m = -2$ são os únicos valores de m possíveis tais que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ seja um domínio Euclidiano com relação a ϕ_m. □

Um resultado análogo ao Teorema 20, com demonstração análoga, vale para $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$.

Teorema 21. *Seja $m \in \mathbb{Z}$ livre de quadrados com $m \equiv 1 \pmod 4$. Então, o domínio de integridade $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ é Euclidiano com respeito a ϕ_m se, e somente se, dados $x, y \in \mathbb{Q}$, existem $a, b \in \mathbb{Z}$ tais que:*

$$\phi_m\left((x + y\sqrt{m}) - \left(a + b\left(\frac{1+\sqrt{m}}{2}\right)\right)\right) < 1$$

Assim como no Teorema 20, podemos usar o resultado anterior para encontrar os valores negativos de m tais que $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ é Euclidiano com relação a ϕ_m, o que nos dá a seguinte proposição:

Proposição 8. *Seja $m \in \mathbb{Z}$ negativo e livre de quadrados, com $m \equiv 1 \pmod 4$. O domínio de integridade $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ é Euclidiano com relação a ϕ_m se, e somente se, $m = -3, -7, -11$.*

Encontrar todos os valores de m positivos que fazem $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ e $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ serem Euclidianos com relação a ϕ_m é menos direto. Entretanto, podemos usar os resultados que conhecemos para mostrar a validade para alguns casos.

Proposição 9. *O domínio de integridade $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com relação a ϕ_m para $m = 2, 3, 6$.*

Demonstração. Provaremos primeiro para $m = 2, 3$. Sejam $x, y \in \mathbb{Q}$. Então existem $a, b \in \mathbb{Z}$ tais que:

$$|x - a| \leq \frac{1}{2} \text{ e } |y - b| \leq \frac{1}{2}$$

Como $(x-a)^2, m(y-b)^2 \geq 0$, temos:

$$\begin{aligned}\phi_m\left(\left(x+y\sqrt{m}\right)-\left(a+b\sqrt{m}\right)\right) &= \phi_m((x-a)+(y-b)\sqrt{m}) \\ &= \left|(x-a)^2 - m(y-b)^2\right| \\ &\leq \max\{|x-a|^2, m|y-b|^2\} \\ &\leq \max\{\frac{1}{4}, \frac{m}{4}\} = \frac{m}{4} \leq \frac{3}{4} < 1\end{aligned}$$

Pelo Teorema 20, segue que $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ é Euclidiano com relação a ϕ_m, para $m = 2, 3$. Suponha agora que $\mathbb{Z}+\mathbb{Z}\sqrt{6}$ não é Euclidiano com respeito a ϕ_6. Pelo Teorema 20, existem $r, s \in \mathbb{Q}$ tais que:

$$\phi_6\left(\left(r+s\sqrt{6}\right)-\left(a+b\sqrt{6}\right)\right) \geq 1 \ \forall a, b \in \mathbb{Z}$$

Ou seja:

$$\left|(r-a)^2 - 6(s-b)^2\right| \geq 1 \ \forall a, b \in \mathbb{Z} \tag{2.3}$$

Sabemos que $\min\{r-\lfloor r\rfloor, -r-\lfloor -r\rfloor\}, \min\{s-\lfloor s\rfloor, -s-\lfloor -s\rfloor\} \leq \frac{1}{2}$. Assim, existem $u_1, u_2 \in \mathbb{Z}$ e $\epsilon_1, \epsilon_2 \in \{-1, 1\}$ tais que:

$$0 \leq \epsilon_1 r + u_1, \epsilon_2 s + u_2 \leq \frac{1}{2}$$

Sejam $r_1 = \epsilon_1 r + u_1, s_1 = \epsilon_2 s + u_2 \in \mathbb{Q}$ e, dados $a, b \in \mathbb{Z}$, sejam $a_1 = \epsilon_1 a + u_1, b_1 = \epsilon_2 b + u_2 \in \mathbb{Z}$ (note que as funções $f, g : \mathbb{Z} \to \mathbb{Z}$, dadas por $f(x) = \epsilon_1 x + u_1$ e $g(x) = \epsilon_2 x + u_2$ são bijetoras). Assim, temos:

$$0 \leq r_1, s_1 \leq \frac{1}{2} \tag{2.4}$$

Ainda, podemos reescrever a propriedade (2.3) como sendo:

$$\begin{aligned}\left|(r-a)^2 - m(s-b)^2\right| &= \left|\epsilon_1^2(r+\epsilon_1 u_1 - (a+\epsilon_1 u_1))^2 - m\epsilon_2^2(s+\epsilon_2 u_2 - (b+\epsilon_2 u_2))^2\right| \\ &= \left|\left(\epsilon_1 r + \epsilon_1^2 u_1 - (a\epsilon_1 + \epsilon_1^2 u_1)\right)^2 - m\left(s\epsilon_2 + \epsilon_2^2 u_2 - (b\epsilon_2 + \epsilon_2^2 u_2)\right)^2\right| \\ &= \left|(\epsilon_1 r + u_1 - (a\epsilon_1 + u_1))^2 - m(s\epsilon_2 + u_2 - (b\epsilon_2 + u_2))^2\right| \\ &= \left|(r_1 - a_1)^2 - m(s_1 - b_1)^2\right| \geq 1 \ \forall a_1, b_1 \in \mathbb{Z}\end{aligned}$$

Tomando $(a, b) = (0, 0), (1, 0), (-1, 0)$ na relação acima:

$$\begin{cases}|r_1^2 - 6s_1^2| \geq 1 \\ \left|(1-r_1)^2 - 6s_1^2\right| \geq 1 \\ \left|(1+r_1)^2 - 6s_1^2\right| \geq 1\end{cases} \tag{2.5}$$

Por outro lado, de (2.4) temos:

$$\begin{cases}\frac{-3}{2} \leq r_1^2 - 6s_1^2 \leq \frac{1}{4} \\ \frac{-5}{4} \leq (1-r_1)^2 - 6s_1^2 \leq 1 \\ \frac{-1}{2} \leq (1+r_1)^2 - 6s_1^2 \leq \frac{9}{4}\end{cases} \tag{2.6}$$

Concatenando (2.5) e (2.6), encontramos que:

$$\frac{-3}{2} \leq r_1^2 - 6s_1^2 \leq -1 \tag{2.7}$$

$$(i)\ (1-r_1)^2 - 6s_1^2 = 1 \text{ ou } (ii)\ \frac{-5}{4} \leq (1-r_1)^2 - 6s_1^2 \leq -1 \tag{2.8}$$

$$1 \leq (1+r_1)^2 - 6s_1^2 \leq \frac{9}{4} \tag{2.9}$$

De (2.7) e (2.9), obtemos:

$$1 \leq 1 + 2r_1 + \left(r_1^2 - 6s_1^2\right) \leq 2r_1 \Rightarrow r_1 \geq \frac{1}{2}$$

Mas sabemos que $r_1 \leq \frac{1}{2}$, donde segue que $r_1 = \frac{1}{2}$. Assim, $(2.8)(i)$ nos dá:

$$\frac{1}{4} - 6s_1^2 = 1 \Rightarrow 6s_1^2 = \frac{-3}{4}$$

O que é impossível. Logo, devemos ter que $(2.8)(ii)$ vale. Assim:

$$\frac{1}{4} - 6s_1^2 \leq -1 \Rightarrow s_1^2 \geq \frac{5}{24}$$

Mas de (2.9) sabemos que $6s_1^2 \leq (1+r_1)^2 - 1 = \frac{5}{4} \Rightarrow s_1^2 \leq \frac{5}{24}$. Portanto, devemos ter $s_1^2 = \frac{5}{24} \Rightarrow s_1 = \pm\sqrt{\frac{5}{24}} \notin \mathbb{Q}$, o que é um absurdo. Dessa forma, $\mathbb{Z} + \mathbb{Z}\sqrt{6}$ é Euclidiano com respeito a ϕ_6. □

Usaremos o teorema anterior e o Teorema 6 para estudar certas equações diofantinas. Antes disso, entretanto, provaremos a seguinte proposição bastante conhecida, que não está presente em (1).

Proposição 10. *Sejam $n, x, y \in \mathbb{Z}$, tais que existem $a, b, c, d \in \mathbb{Z}$ com:*

$$x = a^2 + nb^2$$
$$y = c^2 + nd^2$$

Então existem $u, v \in \mathbb{Z}$ tais que:

$$xy = u^2 + nv^2$$

Demonstração. Por hipótese, temos:

$$\begin{aligned} xy &= \left(a^2 + nb^2\right)\left(c^2 + nd^2\right) = a^2c^2 + n(a^2d^2 + b^2c^2) + n^2b^2d^2 = \\ &= a^2c^2 - 2abcdn + n^2b^2d^2 + n(a^2d^2 + 2abcd + b^2c^2) = \\ &= (ac - nbd)^2 + n\,(ad + bc)^2 \end{aligned}$$

Tomando $u = ac - nbd \in \mathbb{Z}$ e $v = ad + bc \in \mathbb{Z}$, temos:

$$xy = u^2 + nv^2$$

□

Já encontramos critérios para verificar se $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ é Euclidiano com relação a ϕ_m e mostramos alguns casos particulares. Pode-se notar, como foi para o caso de $\mathbb{Z}+\mathbb{Z}\sqrt{6}$, que essa verificação nem sempre é direta ou trivial, mesmo em vista do Teorema 20. Assim, é interessante buscar outras formas de verificar se um domínio de integridade $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ ou $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ não é Euclidiano com relação a ϕ_m, para evitar desprendermos grande esforço utilizando os teoremas já obtidos em casos que podem ser lidados de maneiras mais simples.

Teorema 22. *Seja $m \in \mathbb{Z}$ positivo e livre de quadrados. Se existirem $p, q \in \mathbb{N}$ primos ímpares distintos tais que:*

$$\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$$

e inteiros positivos t, u que satisfazem:

$$pt + qu = m, \;\; p \nmid t, \;\; q \nmid u$$

e um inteiro r tal que:

$$r^2 \equiv pt \pmod{m}$$

Então $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ não é Euclidiano com respeito a ϕ_m.

Demonstração. Suponha que ϕ_m é Euclidiano com respeito a ϕ_m. Então existe $\gamma, \delta \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$ tais que:

$$r\sqrt{m} = m\gamma + \delta, \phi_m(\delta) < \phi_m(m)$$

Fazendo $\gamma = x + y\sqrt{m}$ $(x, y \in \mathbb{Z})$, temos:

$$\phi_m\left(r\sqrt{m} - m\left(x + y\sqrt{m}\right)\right) < \phi_m(m)$$

Isto é:

$$\begin{gathered}\left|m^2x^2 - m(r - my)^2\right| < m^2 \\ m\left|mx^2 - (r - my)^2\right| < m^2 \\ \left|mx^2 - (r - my)^2\right| < m\end{gathered}$$

Como $mx^2 - (r - my)^2 \equiv -r^2 \equiv -pt \pmod{m}$ e $0 < pt < pt + qu = m$, devemos ter:

$$mx^2 - (my - r)^2 = -pt \text{ ou } mx^2 - (my - r)^2 = m - pt = qu$$

Assim, fazendo $X = x$ e $Y = my - r$, temos $mX^2 - Y^2 = -pt$ ou qu. Suponha que $mX^2 - Y^2 = -pt$. Como $\left(\frac{m}{p}\right) = -1$, temos que $p \nmid m$. Ainda, como $p \nmid t$ devemos ter $p \| -pt$. Dessa forma, $p \nmid X, Y$. Logo:

$$\left(\frac{m}{p}\right) = \left(\frac{mX^2}{p}\right) = \left(\frac{Y^2}{p}\right) = 1$$

O que contradiz $\left(\frac{m}{p}\right) = -1$. Suponha então que $mX^2 - Y^2 = qu$. Como $\left(\frac{m}{q}\right) = -1$ temos $q \nmid m$. Ainda, como $q \nmid u$, temos $q \| qu$. Assim, $q \nmid X, Y$ e:

$$\left(\frac{m}{q}\right) = \left(\frac{mX^2}{q}\right) = \left(\frac{Y^2}{q}\right) = 1$$

O que contradiz $\left(\frac{m}{q}\right) = -1$. Portanto, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano com relação a ϕ_m. □

Utilizando o resultado que acabamos de provar, podemos encontrar alguns valores de m para os quais $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano com relação a ϕ_m.

Proposição 11. *$\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano com relação a ϕ_m para $m = 23, 47, 83$.*

Demonstração. O resultado pode ser verificado diretamente utilizando o teorema anterior e as seguintes escolhas para t, u, r, p e q:

m	p	q	t	u	r
23	3	5	1	4	7
47	3	5	4	7	23
83	3	5	1	16	13

□

Um resultado análogo vale para $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$.

Teorema 23. *Seja $m \in \mathbb{Z}$ positivo e livre de quadrados com $m \equiv 1 \pmod 4$. Se existem $p, q \in \mathbb{N}$ primos ímpares distintos tais que:*

$$\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$$

e um inteiro ímpar r tal que:

$$p || (m-1)r^2 - 4m\left[\frac{(m-1)r^2}{4m}\right]$$
$$q || (m-1)r^2 - 4m\left[\frac{(m-1)r^2}{4m}\right] - 4m$$

Então $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ não é Euclidiano com respeito a ϕ_m.

Estudaremos agora um resultado que afirma que, se $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é um domínio Euclidiano com respeito a ϕ_m, sendo $m > 0$ e $m \not\equiv 1 \pmod 4$, então m é limitado (isto é, o conjunto de tais m é finito). Este resultado, em conjunto com a Proposição 7, nos mostra que domínios Euclidianos da forma $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ com respeito a ϕ_m são raros.

Teorema 24. *Seja $m \in \mathbb{Z}$ positivo e livre de quadrados.*

1. *Se $m \equiv 2 \pmod 4$ e $m \geq 42$, então $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano com respeito a ϕ_m.*
2. *Se $m \equiv 3 \pmod 4$ e $m \geq 91$, então $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano com respeito a ϕ_m.*

Demonstração. 1. Como $m \geq 42$ temos $m > 20 + 8\sqrt{6} = 4(\sqrt{3} + \sqrt{2})^2$ de forma que $\sqrt{m} > 2(\sqrt{3} + \sqrt{2})$. Assim:

$$\frac{\sqrt{3m} - 1}{2} - \frac{\sqrt{2m} - 1}{2} = \left(\frac{\sqrt{3} - \sqrt{2}}{2}\right)\sqrt{m} > \left(\frac{\sqrt{3} - \sqrt{2}}{2}\right)2(\sqrt{3} + \sqrt{2}) = 1$$

Assim, existe um inteiro u tal que:

$$\frac{\sqrt{2m} - 1}{2} < u < \frac{\sqrt{3m} - 1}{2}$$

Seja $t = 2u + 1$, de forma que t é um inteiro ímpar satisfazendo:

$$2m < t^2 < 3m$$

Suponha agora que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com respeito a ϕ_m. Então existem $\gamma, \delta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ tais que:

$$t\sqrt{m} = m\gamma + \delta, \phi_m(\delta) < \phi_m(m)$$

Como $\gamma \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, existem $x, y \in \mathbb{Z}$ tais que $\gamma = x + y\sqrt{m}$ e:

$$\phi_m\left(t\sqrt{m} - m\left(x + y\sqrt{m}\right)\right) < \phi_m(m)$$

Isto é:

$$\begin{gathered}\left|m^2x^2 - m(t - my)^2\right| < m^2 \\ m\left|mx^2 - (t - my)^2\right| < m^2 \\ \left|mx^2 - (t - my)^2\right| < m\end{gathered}$$

Sendo $X = t - my, Y = x \in \mathbb{Z}$, temos:

$$\left|X^2 - mY^2\right| < m \text{ e } X^2 - mY^2 \equiv X^2 \equiv t^2 \pmod m$$

Como $2m < t^2 < 3m$, segue que $X^2 - mY^2 = t^2 - 2m$ ou $X^2 - mY^2 = t^2 - 3m$. No primeiro caso, uma vez que $t^2 \equiv 1 \pmod 8$ (uma vez que t é ímpar) e $m \equiv 2 \pmod 4$, temos:

$$X^2 - mY^2 \equiv 5 \pmod 8$$

Logo, X é ímpar (do contrário, $X^2 - mY^2$ não poderia ser ímpar), donde $X^2 \equiv 1 \pmod 8$ e, consequentemente:

$$mY^2 \equiv 4 \pmod 8$$

O que é impossível, pois Y ímpar implica em $Y^2 \equiv 1 \pmod 4 \Rightarrow mY^2 \equiv 2 \pmod 4$ e Y par implica em $2 \mid m$ e $4 \mid Y^2 \Rightarrow 8 \mid mY^2 \Rightarrow mY^2 \equiv 0 \pmod 8$. Em ambos os casos, não temos $mY^2 \equiv 4 \pmod 8$. Dessa forma, devemos ter $X^2 - mY^2 = t^2 - 3m$. Como $t^2 \equiv 1 \pmod 8$, verificamos que:

$$X^2 - mY^2 \equiv 1 - 3m \pmod 8$$

Como m é par, vemos que $X^2 - mY^2$ é ímpar, donde X é ímpar e, assim, $X^2 \equiv 1 \pmod 8$. Logo:

$$m(Y^2 - 3) \equiv 0 \pmod 8$$

E, uma vez que $2||m$, devemos ter que $4 \mid Y^2 - 3 \Rightarrow Y^2 \equiv 3 \pmod 4$, o que é impossível.

2. Como $m \geq 91$ temos $m > 44+8\sqrt{30} = 4(\sqrt{6}+\sqrt{5})^2$, de forma que $\sqrt{m} > 2(\sqrt{6}+\sqrt{5})$. Assim:

$$\frac{\sqrt{6m}-1}{2} - \frac{\sqrt{5m}-1}{2} = \frac{\left(\sqrt{6}-\sqrt{5}\right)}{2}\sqrt{m} > \frac{\left(\sqrt{6}-\sqrt{5}\right)}{2}2(\sqrt{6}+\sqrt{5}) = 1$$

Assim, existe u inteiro tal que:

$$\frac{\sqrt{5m}-1}{2} < u < \frac{\sqrt{6m}-1}{2}$$

Seja $t = 2u + 1$. Então t é um inteiro ímpar que satisfaz $5m < t^2 < 6m$. Suponha que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano com respeito a ϕ_m. Então existem $\gamma, \delta \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$ tais que:

$$t\sqrt{m} = m\gamma + \delta, \phi_m(\delta) < \phi_m(m)$$

Como $\gamma \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, existem $x, y \in \mathbb{Z}$ tais que $\gamma = x + y\sqrt{m}$. Assim:

$$\begin{gathered}
\phi_m(t\sqrt{m} - m(x + y\sqrt{m})) < \phi_m(m) \\
\left|m^2x^2 - m(t - my)^2\right| < m^2 \\
m\left|mx^2 - (t - my)^2\right| < m^2 \\
\left|mx^2 - (t - my)^2\right| < m
\end{gathered}$$

Sejam $X = my - t, Y = x \in \mathbb{Z}$. Então:

$$\left|X^2 - mY^2\right| < m \text{ e } X^2 - mY^2 \equiv X^2 \equiv t^2 \pmod m$$

Como $5m < t^2 < 6m$, devemos ter:

$$X^2 - mY^2 = t^2 - 5m \text{ ou } X^2 - mY^2 = t^2 - 6m$$

No primeiro caso, como $t^2 \equiv 1 \pmod 8$ (pois t é ímpar) e $m \equiv 3 \pmod 4$, temos:

$$X^2 - mY^2 = t^2 - 5m \equiv 1 - 15 \equiv -14 \equiv 2 \pmod 4$$

Como $z^2 \equiv 0$ ou $1 \pmod 4$ para todo $z \in \mathbb{Z}$, a congruência acima nos diz que $X \equiv Y \equiv 1 \pmod 2$. Logo, $X^2 \equiv Y^2 \equiv 1 \pmod 8$, de forma que:

$$1 - 5m \equiv t^2 - 5m = X^2 - mY^2 \equiv 1 - m \pmod 8 \Rightarrow 4m \equiv 0 \pmod 8$$

O que é um absurdo, uma vez que isso implica em m par e $m \equiv 3 \pmod 4 \Rightarrow 2 \nmid m$. Logo, devemos ter $X^2 - mY^2 = t^2 - 6m$. Como $t^2 \equiv 1 \pmod 8$ e $m \equiv 3 \pmod 4$, temos:

$$X^2 - mY^2 = t^2 - 6m \equiv 1 - 18 \equiv -17 \equiv 7 \pmod 8$$

Se X for ímpar, temos $X^2 \equiv 1 \pmod 8 \Rightarrow mY^2 \equiv 2 \pmod 8 \Rightarrow mY^2 \equiv 3Y^2 \equiv 2 \pmod 4 \Rightarrow Y^2 \equiv 2 \pmod 4$, o que é impossível. Se X é par, então $X^2 \equiv 0 \pmod 4$, donde $-mY^2 \equiv -3Y^2 \equiv 3 \pmod 4 \Rightarrow Y^2 \equiv 3 \pmod 4$, o que também é impossível. Portanto, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano com relação a ϕ_m.

□

Os resultados que provamos nos permitem determinar, em alguns casos, se $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ e $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ são Euclidianos ou não com respeito a ϕ_m. Isso, entretanto, não é suficiente para verificar se esses domínios são ou não Euclidianos. De fato, podem haver outras funções que satisfaçam as condições de função euclidiana nesses domínios. Uma maneira de realizar essa verificação é por meio de divisores laterais universais.

Seja D um domínio de integridade. É conveniente definir o conjunto $\widetilde{D} = U(D) \cup \{0\}$, pois assim temos que $D \setminus \widetilde{D} = \emptyset \Leftrightarrow D$ é um corpo.

Definição 20. *Seja D um domínio de integridade que não é um corpo. Um elemento $u \in D \setminus \widetilde{D}$ é chamado de divisor lateral universal se para todo $x \in D$, existir $z \in \widetilde{D}$ tal que $u \mid x - z$.*

Teorema 25. *Seja D um domínio de integridade que não é um corpo. Se D não possui divisores laterais universais, então D não é Euclidiano.*

Demonstração. Suponha que D seja Euclidiano com respeito a uma função ϕ e que não tenha divisores laterais universais. Seja $S = \{\phi(v) \mid v \in D \setminus \widetilde{D}\} \subset \mathbb{Z}$. Como D não é corpo, $D \setminus \widetilde{D} \neq \emptyset$, donde $S \neq \emptyset$. Pelo item 2 do Teorema 17, sabemos que S é limitado inferiormente por $\phi(0)$. Pelo PBO, S possui um menor elemento $\phi(u)$, com $u \in D \setminus \widetilde{D}$. Como D é Euclidiano com respeito a ϕ, para todo $x \in D$ existem $y, z \in D$ tais que $x = uy + z$ e $\phi(z) < \phi(u)$. Se $z = 0$ então $x = uy \Rightarrow u \mid x$. Se $z \neq 0$, pela minimalidade de $\phi(u)$, devemos ter $z \in U(D)$. Em ambos os casos, temos $u \mid x - z$ para algum $z \in \widetilde{D}$. Logo, para todo $x \in D$, existe $z \in \widetilde{D}$ tal que $u \mid x - z$. Por definição, u é um divisor lateral universal, o que contradiz D não possuir divisores laterais universais. □

Com este resultado, podemos provar que, para certos valores de m, $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ e $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ não são domínios Euclidianos. Para isso, necessitaremos dos dois próximos lemas.

Lema 2. *Seja $m \in \mathbb{Z}^*_-$ livre de quadrados. Se $m < -1$, temos $U(\mathbb{Z}+\mathbb{Z}\sqrt{m}) = \{-1, 1\}$.*

Demonstração. Primeiramente, $(-1)\times(-1) = 1$ e $1\times 1 = 1$, donde $\{-1, 1\} \subset U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$. Por outro lado, seja $a \in U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$. Então, existem $x, y \in \mathbb{Z}$ tais que $x+y\sqrt{m} \mid 1$. Usando as propriedades de ϕ_m, temos:

$$\left|x^2-my^2\right| = \phi_m\left(x+y\sqrt{m}\right) \mid \phi_m(1) = 1 \Rightarrow \left|x^2-my^2\right| = \pm 1 \text{ e } \left|x^2-my^2\right| \geq 0$$
$$\Rightarrow \left|x^2-my^2\right| = 1 \Rightarrow x^2-my^2 = \pm 1$$

Como $m < -1$, temos $m \leq -2 \Rightarrow -m \geq 2 \Rightarrow x^2-my^2 \geq x^2+2y^2 \geq 0$, donde $x^2-my^2 = 1$. Suponha $y \neq 0$. Então $|y| \geq 1 \Rightarrow y^2 = |y|^2 \geq 1 \Rightarrow 1 = x^2-my^2 \geq x^2+2y^2 \geq 2y^2 \geq 2 > 1$ (absurdo). Assim, $y = 0$ e $x^2 = 1 \Rightarrow x = \pm 1$, donde $x+y\sqrt{m} = \pm 1$. Logo, $U(\mathbb{Z}+\mathbb{Z}\sqrt{m}) \subset \{-1, 1\}$. Como a inclusão inversa já foi provada, temos $U(\mathbb{Z}+\mathbb{Z}\sqrt{m}) = \{-1, 1\}$. □

Lema 3. *Seja $m \in \mathbb{Z}$ negativo e livre de quadrados. Se $p \in \mathbb{Z}$ é primo e $m < -p$, então p é irredutível em $\mathbb{Z}+\mathbb{Z}\sqrt{m}$.*

Demonstração. Seja $a \in \mathbb{Z}+\mathbb{Z}\sqrt{m} \setminus U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$ tal que $a \mid p$. Como $a \in \mathbb{Z}+\mathbb{Z}\sqrt{m}$, existem $x, y \in \mathbb{Z}$ tais que $a = x+y\sqrt{m}$. Usando as propriedades de ϕ_m, temos:

$$x+y\sqrt{m} \mid p \Rightarrow \phi_m\left(x+y\sqrt{m}\right) \mid \phi_m(p) \Rightarrow \left|x^2-my^2\right| \mid p^2$$

Ainda, como $m < -p$, temos $m \leq -p-1 \Rightarrow -m \geq p+1 \Rightarrow x^2-my^2 \geq x^2+(p+1)y^2 \geq x^2+(2+1)y^2 = x^2+3y^2 \geq 0$. Assim, x^2-my^2 é um divisor positivo de p^2, ou seja, $x^2-my^2 = 1, p$ ou p^2.

- Caso $x^2-my^2 = 1$: Neste caso, suponha que $y \neq 0$. Então $y^2 \geq 1 \Rightarrow 1 = x^2-my^2 \geq x^2+3y^2 \geq 3y^2 \geq 3 > 1$ (absurdo). Logo, $y = 0$ e $x^2 = 1 \Rightarrow x = \pm 1$, donde $x+y\sqrt{m} = \pm 1 \in U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$, o que contradiz $x+y\sqrt{m} \in \mathbb{Z}+\mathbb{Z}\sqrt{m} \setminus U(\mathbb{Z}+\mathbb{Z}\sqrt{m})$.

- Caso $x^2-my^2 = p$: Suponha que $y \neq 0$. Então $y^2 \geq 1 \Rightarrow p = x^2-my^2 \geq x^2+(p+1)y^2 \geq (p+1)y^2 \geq p+1 > p$ (absurdo). Logo, $y = 0$ e $x^2 = p \Rightarrow x = \pm\sqrt{p} \notin \mathbb{Z}$, o que é uma contradição.

- Caso $x^2-my^2 = p^2$: Neste caso, como $x+y\sqrt{m} \mid p$, existem $u, v \in \mathbb{Z}$ tais que $(x+y\sqrt{m})(u+v\sqrt{m}) = p$. Assim, usando as propriedades de ϕ_m, temos $\phi_m\left((x+y\sqrt{m})(u+v\sqrt{m})\right) = \phi_m(x+y\sqrt{m})\,\phi_m(u+v\sqrt{m}) = p^2\phi_m(u+v\sqrt{m}) = \phi_m(p) = p^2 \Rightarrow \phi_m(u+v\sqrt{m}) = 1$. Pelo que mostramos no primeiro caso, isso implica em $u+v\sqrt{m} = \pm 1 \Rightarrow x+y\sqrt{m} = \pm p \sim p$.

Logo, $x + y\sqrt{m} \mid p$ e $x + y\sqrt{m} \notin U(\mathbb{Z} + \mathbb{Z}\sqrt{m})$ implica em $x + y\sqrt{m} \sim p$. Por definição, temos que p é irredutível em $\mathbb{Z} + \mathbb{Z}\sqrt{m}$. □

Com isso, podemos mostrar que, para certos valores m, $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é domínio Euclidiano.

Teorema 26. *Seja $m \in \mathbb{Z}$ negativo e livre de quadrados. Se $m \equiv 2, 3 \pmod 4$ e $m < -2$, então $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano.*

Demonstração. Seja $D = \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Note que D é um domínio de integridade que não é corpo. Como $m \neq -1$, temos $U(D) = \{-1, 1\}$. Com isso, sabemos que $\widetilde{D} = \{0, -1, 1\}$. Suponha que u é um divisor lateral universal em D. Então u deve dividir $2 - 1, 2 + 0$ ou $2 + 1$, isto é, u deve dividir $1, 2$ ou 3. Mas $u \nmid 1$, pois u não é uma unidade. Assim, $u \mid 2$ ou $u \mid 3$. Como $m \equiv 2, 3 \pmod 4$ e $m < -2$, temos $m \leq -5$, donde 2 e 3 são irredutíveis em $\mathbb{Z}+\mathbb{Z}\sqrt{m}$. Portanto, as únicas possibilidades para u são $2, 3, -2$ e -3. Como u é um divisor lateral universal e $\sqrt{m} \in D$, existe $z \in \widetilde{D}$ tal que $u \mid \sqrt{m} - z$. Isto é, $u \mid \sqrt{m} - 1$, $u \mid \sqrt{m}$ ou $u \mid \sqrt{m} + 1$. Entretanto, note que, dados $x, y \in \mathbb{Z}$, temos $2(x + y\sqrt{m}) = 2x + 2y\sqrt{m}$ e $3(x + y\sqrt{m}) = 3x + 3y\sqrt{m}$. Assim, se $a + b\sqrt{m} \in D$, temos $2 \mid a + b\sqrt{m} \Rightarrow 2 \mid b$ e $3 \mid a + b\sqrt{m} \Rightarrow 3 \mid b$. Como $2, 3 \nmid 1$, temos que $2, 3 \nmid \sqrt{m} - 1, \sqrt{m}, \sqrt{m} + 1$. Ainda, como $3 \mid a + b\sqrt{m} \Leftrightarrow -3 \mid a + b\sqrt{m}$ e $2 \mid a + b\sqrt{m} \Leftrightarrow -2 \mid a + b\sqrt{m}$, temos $-2, -3 \nmid \sqrt{m} - 1, \sqrt{m}, \sqrt{m} + 1$. Portanto, $u \neq -3, -2, 2, 3$. Uma vez que essas eram as únicas possibilidades para u, segue que $D = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ não possui divisores laterais universais. Pelo teorema anterior, segue que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ não é Euclidiano. □

É possível demonstrar lemas semelhantes para $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, e com eles chegar a um resultado análogo ao anterior para esses domínios.

Lema 4. *Seja $m \in \mathbb{Z}$ livre de quadrados, com $m \equiv 1 \pmod 4$ e $m < -3$. Então, $U\left(\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)\right) = \{-1, 1\}$.*

Lema 5. *Sejam $p \in \mathbb{Z}$ primo, $m \in \mathbb{Z}$ livre de quadrados, com $m \equiv 1 \pmod 4$ e $m < -4p$. Então p é irredutível em $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$.*

Teorema 27. *Seja $m \in \mathbb{Z}$ livre de quadrados com $m \equiv 1 \pmod 4$ e $m < -11$. Então $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ não é Euclidiano.*

Usaremos alguns dos resultados já apresentados para obter representações de primos como formas quadráticas binárias. Para isso, usaremos os Teoremas 6 e 7, além da seguinte proposição, conhecida da teoria dos números:

Proposição 12. *Seja $p \in \mathbb{Z}$ um primo ímpar. Então:*

$$\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4$$
$$\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \equiv 1, 3 \pmod 8$$
$$\left(\frac{-3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 3$$
$$\left(\frac{-7}{p}\right) = 1 \Leftrightarrow p \equiv 1, 2, 4 \pmod 7$$
$$\left(\frac{-11}{p}\right) = 1 \Leftrightarrow p \equiv 1, 3, 4, 5, 9 \pmod{11}$$

Uma demonstração para os casos -1 e -2 pode ser encontrada em (2). A demonstração dos demais casos é análoga.

Teorema 28. *Seja $p \in \mathbb{Z}$ um primo tal que $p \equiv 1 \pmod 4$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + y^2$.*

Demonstração. Como $p \equiv 1 \pmod 4$, pela proposição 12 temos $\left(\frac{-1}{p}\right) = 1$. Como $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$ é um domínio Euclidiano, pelo Teorema 18, temos $\mathbb{Z} + \mathbb{Z}\sqrt{-1}$ domínio de ideais principais. Logo, pelo Teorema 6, existem inteiros $x, y \in \mathbb{Z}$ tais que $p = x^2 + y^2$. □

Teorema 29. *Seja $p \in \mathbb{Z}$ um primo tal que $p \equiv 1, 3 \pmod 8$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + 2y^2$.*

A demonstração desse resultado é análoga à do teorema anterior.

Teorema 30. *Seja $p \in \mathbb{Z}$ um primo tal que $p \equiv 1 \pmod 3$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + xy + y^2$.*

Demonstração. Como $p \equiv 1 \pmod 3$, pela proposição 12 temos $\left(\frac{-3}{p}\right) = 1$. Como $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$ é um domínio Euclidiano, pelo Teorema 18, temos $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-3}}{2}\right)$ domínio de ideais principais. Logo, pelo Teorema 7, existem inteiros $x, y \in \mathbb{Z}$ tais que $p = x^2 + xy + y^2$. □

Com demonstração análoga à do último teorema, encontramos também os seguintes resultados:

Teorema 31. *Seja $p \in \mathbb{Z}$ um primo tal que $p \equiv 1, 2, 4 \pmod 7$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + xy + 2y^2$.*

Teorema 32. *Seja $p \in \mathbb{Z}$ um primo tal que $p \equiv 1, 3, 4, 5, 9 \pmod{11}$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 + xy + 3y^2$.*

Ainda, mostramos que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é Euclidiano para $m = 2, 3, 6$. Pela teoria dos números, sabemos que para um primo ímpar p, temos:

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv 1, 7 \pmod 8$$
$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv 1, 11 \pmod{12}$$
$$\left(\frac{6}{p}\right) = 1 \Leftrightarrow p \equiv 1, 5, 19, 23 \pmod{24}$$

Utilizando este fato e o Teorema 6, temos:

Teorema 33. *Seja p um primo tal que $p \equiv 1, 7 \pmod 8$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 - 2y^2$.*

Demonstração. Como $p \equiv 1, 7 \pmod 8$, sabemos que $\left(\frac{2}{p}\right) = 1$. Como $\mathbb{Z}+\mathbb{Z}\sqrt{2}$ é domínio Euclidiano, temos pelo Teorema 18 que $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ é domínio de ideais principais. Pelo Teorema 6, como existem $T = U = 1$ tais que $T^2 - 2U^2 = -1$, segue que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 - 2y^2$. □

Teorema 34. *Seja p um primo tal que $p \equiv 1, 11 \pmod{12}$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 - 3y^2$ ou $p = 3y^2 - x^2$.*

Demonstração. Como $p \equiv 1, 11 \pmod{12}$, sabemos que $\left(\frac{3}{p}\right) = 1$. Como $\mathbb{Z} + \mathbb{Z}\sqrt{3}$ é domínio Euclidiano, temos pelo Teorema 18 que $\mathbb{Z} + \mathbb{Z}\sqrt{3}$ é domínio de ideais principais. Pelo Teorema 6, como não existem $T, U \in \mathbb{Z}$ tais que $T^2 - 3U^2 = -1$ (de fato, $T^2 - 3U^2 = -1 \Rightarrow T^2 \equiv -1 \equiv 2 \pmod 3$, o que é um absurdo), segue que existem $x, y \in \mathbb{Z}$ tais que $p = x^2 - 3y^2$ ou $p = 3y^2 - x^2$. □

Teorema 35. *Seja p um primo tal que $p \equiv 1, 5, 19, 23 \pmod{24}$. Então existem $x, y \in \mathbb{Z}$ tais que $p = x^2 - 6y^2$ ou $p = 6y^2 - x^2$.*

A demonstração desse último resultado é análoga à do teorema anterior.

Por fim, note que, com a Proposição 10, os Teoremas 28, 29 e 33 implicam que, se todos os divisores primos de k são das formas mencionadas nos enunciados destes teoremas, então a equação $k = x^2 + ny^2$ possui solução (sendo n o mesmo do enunciado destes teoremas). Ainda, os Teoremas 34 e 35 implicam que se todos os divisores primos de k são das formas mencionadas nos enunciados destes teoremas, então a equação $k = x^2 + ny^2$ ou a equação $-k = x^2 + ny^2$ possui solução (sendo n o mesmo do enunciado destes teoremas).

2.5 DOMÍNIOS NOETHERIANOS

Seja $I \subset \mathbb{Z}$ um ideal. Como $\mathbb{Z}$ é um domínio de ideais principais, existe $m \in \mathbb{Z}$ tal que $I = \langle m \rangle$. Considere agora um ideal $J \subset I$. Sabemos que existe $n \in \mathbb{Z}$ tal que $J = \langle n \rangle$. Pela Proposição 3, sabemos que $m \mid n$. Como n possui um número finito de divisores, existe uma quantidade finita de ideais I' distintos tais que $J \subset I'$. Em particular, não existem infinitos ideais I_k de $\mathbb{Z}$, com $k \in \mathbb{N}$, tais que:

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq ...$$

Esta propriedade, como veremos mais adiante, não vale para todos os domínios de integridade. Além disso, veremos também que os domínios que satisfazem esta propriedade possuem características importantes.

Comecemos formalizando nossas observações acima.

Definição 21 (Cadeia ascendente de ideais)**.** *Uma sequência $(I_n)_{n\in\mathbb{N}}$ de ideais em um domínio de integridade é dita uma cadeia ascendente de ideais se:*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$$

A sequência é dita estritamente ascendente se:

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq ... \subsetneq I_n \subsetneq ...$$

Definição 22. *Dizemos que uma cadeia ascendente de ideais $(I_n)_{n\in\mathbb{N}}$ termina se existe um inteiro positivo n_0 tal que $I_n = I_{n_0}$ para todo $n \geq n_0$.*

Podemos agora definir o que é um domínio Noetheriano.

Definição 23 (Domínio Noetheriano)**.** *Um domínio de integridade D tem a propriedade da cadeia ascendente se toda cadeia ascendente de ideais em D termina. Equivalentemente, D tem a propriedade da cadeia ascendente se D não contém uma cadeia estritamente ascendente de ideais. Um domínio com essa propriedade é chamado de domínio Noetheriano.*

Começaremos dando a definição de condição maximal e mostrando algumas equivalências.

Definição 24 (Condição maximal)**.** *Um domínio de integridade D satisfaz a condição maximal se, para todo conjunto não-vazio S de ideais de D, existe $I \in S$ tal que, se $J \in S$ e $I \subseteq J$, então $I = J$ (dizemos que I é o elemento maximal de S).*

Teorema 36. *Seja D um domínio de integridade. São equivalentes:*

1. *D é Noetheriano.*

2. *D satisfaz a condição maximal.*

3. *Todo ideal de D é finitamente gerado.*

Demonstração.

- $(1. \Rightarrow 2.)$: Suponha que D é um domínio Noetheriano que não satisfaz a condição maximal. Então D possui um conjunto $S \neq \emptyset$ de ideais de D tal que, para todo ideal $I \in S$, existe $J \in S$ tal que $I \subsetneq J$. Assim, como $S \neq \emptyset$, existe $I_1 \in S$. Dado que $I_1 \in S$, existe $I_2 \in S$ tal que $I_1 \subsetneq I_2$. Suponha que exista $n \in \{2, 3, 4, ...\}$ tal que $I_1 \subsetneq I_2 \subsetneq ... \subsetneq I_n$, com $I_1, I_2, ..., I_n \in S$. Como $I_n \in S$, existe $I_{n+1} \in S$ tal que $I_n \subsetneq I_{n+1}$. Assim, $I_1, I_2, ..., I_n, I_{n+1} \in S$ e $I_1 \subsetneq I_2 \subsetneq ...I_n \subsetneq I_{n+1}$. Pelo Princípio da Indução, existe $(I_n)_{n\in\mathbb{N}} \subset S$ tal que $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq ... \subsetneq I_n \subsetneq ....$ Logo, $(I_n)_{n\in\mathbb{N}}$ é uma cadeia estritamente ascendente de ideais, o que contradiz D ser Noetheriano.

- $(2. \Rightarrow 3.)$: Suponha que D seja um domínio que satisfaz a condição maximal e que exista $I \subset D$ um ideal que não é finitamente gerado. Então $I \neq \{0\}$, pois $\{0\} = \langle 0 \rangle$. Assim, existe $a_1 \in I \setminus \{0\}$, donde $\langle a_1 \rangle = I_1 \subset I$. Como $I = I_1$ implicaria em I finitamente gerado, temos $I \neq I_1$. Assim, existe $a_2 \in I \setminus I_1$. Sendo $I_2 = \langle a_1, a_2 \rangle$, temos $I_1 \subsetneq I_2 \subset I$. Suponha que, para $n \in \{2, 3, 4, ...\}$, existam $a_1, ..., a_n \in I$ tais que, se $I_k = \langle a_1, ..., a_k \rangle$ para todo $k \in \{1, ..., n\}$, temos $I_1 \subsetneq I_2 \subsetneq ... \subsetneq I_n \subset I$. Sabemos que $I \neq I_n$, pois I_n é finitamente gerado. Logo, existe $a_{n+1} \in I \setminus I_n$. Sendo $I_{n+1} = \langle a_1, a_2, ..., a_n, a_{n+1} \rangle$, temos $I_1 \subsetneq I_2 \subsetneq ... \subsetneq I_n \subsetneq I_{n+1} \subset I$. Pelo Princípio de Indução, existe $(I_n)_{n\in\mathbb{N}}$ sequência de ideais em D tais que $I_1 \subsetneq I_2 \subsetneq ... \subsetneq I_n \subsetneq ....$ Seja $S = \{I_n \mid n \in \mathbb{N}\} \neq \emptyset$ um conjunto de ideais de D. Dado $I_n \in S$, existe $I_{n+1} \in S$ tal que $I_n \subsetneq I_{n+1}$. Logo, S não possui um ideal I tal que, se $J \in S$ e $I \subseteq J$, então $I = J$, o que contradiz D satisfazer a condição maximal.

- $(3. \Rightarrow 1.)$: Seja $I_1 \subseteq I_2 \subseteq I_3 \subseteq ... \subseteq I_n \subseteq ...$ uma cadeia ascendente de ideais em D. Seja $I = \bigcup\limits_{n\in\mathbb{N}} I_n$. Dados $a, b \in I$ e $r \in D$, temos que existem $m, n \in \mathbb{N}$ tais que $a \in I_m$ e $b \in I_n$. Sendo $k = \max\{m, n\} \in \mathbb{N}$, temos $I_m, I_n \subseteq I_k \Rightarrow a, b \in I_k \Rightarrow a+b \in I_k \subset I$. Ainda, $a \in I_m \Rightarrow ra \in I_m \subset I$. Portanto, I é ideal de D. Logo, I é finitamente gerado. Sejam $a_1, a_2, ..., a_l \in D$ geradores de I (isto é, $I = \langle a_1, a_2, ..., a_l \rangle$). Dado $i \in \{1, ..., l\}$, temos que $a_i \in I = \bigcup\limits_{n\in\mathbb{N}} I_n$, donde existe $n_i \in \mathbb{N}$ tal que $a_i \in I_{n_i}$. Tomando $n_0 = \max\{n_1, n_2, ..., n_l\} \in \mathbb{N}$, temos que $a_i \in I_{n_i} \subset I_{n_0}$ para todo $i \in \{1, ..., l\}$, donde $I = \langle a_1, ..., a_l \rangle \subseteq I_{n_0} \subseteq \bigcup\limits_{n\in\mathbb{N}} I_n = I \Rightarrow I = I_{n_0}$. Assim, se $s \geq n_0$, temos $I_{n_0} \subseteq I_s \subseteq I = I_{n_0} \Rightarrow I_s = I_{n_0}$, donde a cadeia ascendente de ideais termina. Como esta cadeia foi tomada arbitrariamente em D, temos que toda cadeia ascendente de ideais em D termina, isto é, D é Noetheriano.

□

Como consequência deste resultado, temos o seguinte corolário:

Corolário 2. *Todo domínio de ideais principais é um domínio Noetheriano.*

Demonstração. Seja D um domínio de ideais principais. Então todo ideal de D é principal e, portanto, finitamente gerado. Pelo resultado anterior, isso implica em D domínio Noetheriano. □

Exemplo 5. *Mostremos que nem todo domínio de integridade é Noetheriano. De fato, se F é um corpo, então $F[X_1, X_2, X_3, ...]$ é um domínio de integridade. Ainda, vale que:*

$$\langle X_1 \rangle \subset \langle X_1, X_2 \rangle \subset \langle X_1, X_2, X_3 \rangle \subset ...$$

donde $F[X_1, X_2, X_3, ...]$ não é um domínio Noetheriano. Em particular, $F[X_1, X_2, X_3, ...]$ não é um domínio de ideais principais, pelo resultado anterior.

2.6 DOMÍNIOS DE FATORAÇÃO E DOMÍNIOS DE FATORAÇÃO ÚNICA

Assim como fizemos para domínios Euclidianos, domínios de ideais principais e domínios Noetherianos, definiremos mais um tipo de domínio, os domínios de fatoração, baseado em uma das propriedades dos números inteiros: a propriedade de que todo inteiro não-nulo que não é uma unidade pode ser escrito como produto finito de irredutíveis.

Definição 25 (Domínio de fatoração)**.** *Seja D um domínio de integridade. Então D é dito um domínio de fatoração se todo $u \in D \setminus \widetilde{D}$ pode ser expresso como um produto finito de irredutíveis de D.*

Provaremos agora uma proposição e, em seguida, mostraremos que todo domínio Noetheriano é também um domínio de fatoração.

Proposição 13. *Seja D um domínio de integridade que não é um corpo. Se D é Noetheriano então D contém elementos irredutíveis.*

Demonstração. Suponha que exista D domínio Noetheriano que não é corpo e não contém irredutíveis. Como D não é corpo, $D \setminus \widetilde{D} \neq \emptyset$. Assim, seja $a_1 \in D \setminus \widetilde{D}$. Sabemos que a_1 não é irredutível, isto é, a_1 é redutível. Logo, existe $a_2 \in D \setminus \widetilde{D}$ tal que $a_2 \mid a_1$ e $a_2 \not\sim a_1$. Pela Proposição 3, temos $\langle a_1 \rangle \subsetneq \langle a_2 \rangle$. Seja $n \in \mathbb{N}$ tal que $a_1, a_2, ..., a_n \in D \setminus \widetilde{D}$ e $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq ... \subsetneq \langle a_n \rangle$. Sabemos que a_n não é irredutível. Assim, existe $a_{n+1} \in D \setminus \widetilde{D}$ tal que $a_{n+1} \mid a_n$ e $a_{n+1} \not\sim a_n$. Pela Proposição 3, temos $\langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq ... \subsetneq \langle a_n \rangle \subsetneq \langle a_{n+1} \rangle$. Pelo Princípio de Indução, segue que $(\langle a_n \rangle)_{n \in \mathbb{N}}$ é uma cadeia estritamente ascendente de ideais em D, o que contradiz D ser Noetheriano. □

Teorema 37. *Todo domínio Noetheriano é um domínio de fatoração.*

Demonstração. Seja D um domínio Noetheriano e suponha que D não é um domínio de fatoração. Então D contém pelo menos um elemento $u \in D \setminus \widetilde{D}$ que não é um produto finito de irredutíveis de D. Seja A o conjunto desses elementos. Assim, $A \neq \emptyset$. Seja:

$$S = \{\langle a\rangle \mid a \in A\}$$

Temos $S \neq \emptyset$. Como D é Noetheriano, pela condição maximal, S possui um elemento maximal $\langle b\rangle, b \in A$. Assim, $b \in D \setminus \widetilde{D}$ e b não é um produto finito de irredutíveis. Logo, b não é irredutível. Portanto, podemos escrever $b = cd$, com $c, d \in D \setminus \widetilde{D}$. Assim, pela Proposição 3, temos $\langle b\rangle = \langle cd\rangle \subseteq \langle c\rangle, \langle d\rangle$. Ainda, como $c, d \notin U(D)$, temos $c, d \not\sim b$, donde $\langle b\rangle \subsetneq \langle c\rangle, \langle d\rangle$. Pela maximalidade de $\langle b\rangle$, temos $\langle c\rangle, \langle d\rangle \notin S$. Logo, c e d são produtos finitos de irredutíveis, donde $b = cd$ é produto finito de irredutíveis, o que é um absurdo. Assim, D é um domínio de fatoração. □

Seja D um domínio de fatoração e $a \in D \setminus \widetilde{D}$. Então existem irredutíveis $h_1, h_2, ..., h_k \in D$ tais que:

$$a = h_1 h_2 ... h_k$$

Se $h_1 \sim h_2$, donde $h_2 = vh_1$, $v \in U(D)$, então:

$$a = vh_1^2 h_3 ... h_k$$

Repetindo esse processo, chegamos a uma fatoração de a da forma:

$$a = wl_1^{k_1} ... l_m^{k_m}$$

em que $w \in U(D)$, $k_i > 0$ e l_i é irredutível para todo $i \in \{1, ..., m\}$ e $i, j \in \{1, ..., m\}$ com $i \neq j$ implica $l_i \not\sim l_j$. A partir de agora, ao nos referirmos a uma fatoração de a, estaremos considerando uma fatoração desta forma.

Definição 26 (Fatoração única)**.** *Sejam D um domínio de fatoração, $a \in D \setminus \widetilde{D}$ e $a = wl_1^{k_1} ... l_m^{k_m}$ uma fatoração de a. Se sempre que considerarmos uma outra fatoração $a = uh_1^{j_1} ... h_n^{j_n}$ tivermos $m = n$ e, após um rearranjo de $h_1, ..., h_m$, tivermos $l_1 \sim h_1, ..., l_m \sim h_m$ e $k_1 = j_1, ..., k_m = j_m$, dizemos que a possui fatoração única.*

Note que a definição acima é bastante semelhante à propriedade descrita pelo Teorema Fundamental da Aritmética, o qual é um dos resultados mais importantes referentes aos números inteiros. Isso nos leva a definir outro tipo de domínio, e a investigar suas propriedades:

Definição 27 (Domínio de fatoração única)**.** *Seja D um domínio de fatoração. Se todo $u \in D \setminus \widetilde{D}$ possui fatoração única, dizemos que D é um domínio de fatoração única.*

É evidente que todo domínio de fatoração única é também um domínio de fatoração. Entretanto, veremos que a recíproca não é verdadeira.

Provaremos alguns resultados referente aos domínios de fatoração única.

Lema 6. *Seja D um domínio de fatoração e $p \in D$ primo. Então p possui fatoração única.*

Demonstração. Seja $p = uh_1^{j_1}...h_k^{j_k}$ uma fatoração de p, com $u \in U(D)$, $h_1, ..., h_k$ irredutíveis, $j_1, ..., j_k \in \mathbb{N}$ e $h_i \not\sim h_j$ para $i \neq j$. Como p é primo e $p \mid uh_1^{j_1}...h_k^{j_k}$, temos que $p \mid h_s$ para algum $1 \leq s \leq n$ (note que $p \nmid u$ pois p primo implica em $p \notin U(D)$). Reordenando os $h's$ se necessário, podemos supor que $p \mid h_1$. Como h_1 é irredutível, segue que $p \sim h_1$. Logo, existe $v \in U(D)$ tal que $h_1 = pv$, donde:

$$1 = \frac{p}{p} = uvh_1^{j_1-1}...h_k^{j_k}$$

Se $k > 1$, então $j_2 \in \mathbb{N}$ implica em $h_2 \mid uvh_1^{j_1-1}...h_k^{j_k} = 1$, donde $h_2 \in U(D)$, o que contradiz h_2 irredutível. Logo $k = 1$ e $1 = uvh_1^{j_1-1}$. Como $j_1 \in \mathbb{N}$, se $j_1 - 1 \neq 0$, temos $j_1 - 1 \in \mathbb{N}$, donde $h_1 \mid uvh_1^{j_1-1} = 1 \Rightarrow h_1 \in U(D)$, o que contradiz h_1 ser irredutível. Portanto, $j_1 - 1 = 0$, isto é, $j_1 = 1$ e $p = uh_1$, com $p \sim h_1$. Assim, p possui fatoração única. □

Teorema 38. *Seja D um domínio de ideais principais. Então D é um domínio de fatoração única.*

Demonstração. Seja D um domínio de ideais principais. Pelo Corolário 2, D é um domínio Noetheriano e, pelo Teorema 37, D é um domínio de fatoração. Suponha que D não é um domínio de fatoração única. Então existe $a \in D \setminus \widetilde{D}$ que possui duas fatorações distintas como produto de irredutíveis de D. Seja A o conjunto de todos esses elementos, e seja:

$$S = \{\langle a \rangle \mid a \in A\}$$

Como $A \neq \emptyset$ (pois $a \in A$), temos $S \neq \emptyset$. Como D é domínio Noetheriano, sabemos que S possui um elemento maximal $\langle b \rangle$, $b \in A$. Assim, b possui duas fatorações diferentes como produto de irredutíveis de D, isto é:

$$b = ul_1^{k_1}...l_m^{k_m} = vh_1^{j_1}...h_n^{j_n}$$

em que $u, v \in U(D)$, $l_1, ..., l_m, h_1, ..., h_n$ irredutíveis de D, $k_1, ..., k_m, j_1, ..., j_n \in \mathbb{N}$, $l_i \not\sim l_j$ e $h_i \not\sim h_j$ para $i \neq j$. Como $k_1 > 0$, vemos que $l_1 \mid b$, e então $l_1 \mid vh_1^{j_1}...h_n^{j_n}$. Como D é domínio de ideais principais e l_1 é irredutível, pelo Teorema 4, temos l_1 primo. Como $l_1 \nmid v$ (pois $l_1 \notin U(D)$), temos que $l_1 \mid h_s$ para algum inteiro s com $1 \leq s \leq n$. Reordenando os índices dos $h's$, se necessário, podemos supor que $l_1 \mid h_1$. Como l_1 e h_1 são ambos irredutíveis, devemos ter $l_1 \sim h_1$, donde $h_1 = l_1 w$, em que w é uma unidade de D. Assim:

$$\frac{b}{l_1} = ul_1^{k_1-1}...l_m^{k_m} = vwh_1^{j_1-1}...h_n^{j_n}$$

Como l_1 não é uma unidade, temos $\langle b \rangle \subsetneq \left\langle \frac{b}{l_1} \right\rangle$. Então, pela maximalidade de $\langle b \rangle$, temos que $\left\langle \frac{b}{l_1} \right\rangle \notin S \Rightarrow \frac{b}{l_1} \notin A$. Note que $\frac{b}{l_1} \neq 0$, pois $b \neq 0$. Ainda, note que se $\frac{b}{l_1} \in U(D)$,

então $b = ul_1$, com $u \in U(D)$. Pelo lema anterior, l_1 possui fatoração única, donde b possui fatoração única, o que é um absurdo. Logo, $\frac{b}{l_1} \notin U(D)$, isto é, $\frac{b}{l_1} \in D \setminus \widetilde{D}$. Como $\frac{b}{l_1} \notin A$, temos pela definição de A que $\frac{b}{l_1}$ possui fatoração única. Assim, após uma reordenação dos $h's$, se necessário, temos:

$$m = n$$
$$k_1 - 1 = j_1 - 1, k_2 = j_2, ..., k_m = j_m \Rightarrow k_1 = j_1, k_2 = j_2, ..., k_m = j_m$$
$$l_1 \sim h_1, l_2 \sim h_2, ..., l_m \sim h_m$$

o que contradiz a hipótese de que b possui duas fatorações distintas. Portanto, D é um domínio de fatoração única. □

Podemos agora provar uma versão mais forte do Teorema 4:

Teorema 39. *Seja D um domínio de fatoração única. Um elemento de D é irredutível se, e somente se, ele é primo.*

Demonstração. Seja p um irredutível de D. Suponha que $p \mid ab$, em que $a, b \in D$. Então existe $c \in D$ tal que $ab = pc$. Como D é um domínio de fatoração, temos:

$$a = p_1...p_l, b = q_1...q_m, c = r_1...r_n$$

em que $p_1, ..., p_l, q_1, ..., q_m, r_1, ..., r_n$ são irredutíveis de D não necessariamente distintos. Então:

$$p_1...p_l q_1...q_m = pr_1...r_n$$

Como D é um domínio de fatoração única, p deve ser associado a algum p_i ou q_j, donde $p \mid a$ ou $p \mid b$. Assim, p é primo.

Como p primo implica em p irredutível para domínios de integridade no geral, o resultado segue. □

2.7 MÓDULOS

A ideia por trás dos módulos é a de criar uma estrutura algébrica sobre anéis de maneira análoga à estrutura de espaços vetoriais sobre corpos. Para isso, devemos antes definir uma ação de um anel sobre um grupo.

Definição 28 (R-ação)**.** *Sejam R um anel com identidade e M um grupo abeliano aditivo. Uma função $\alpha : R \times M \to M$ é chamada uma R-ação em M se α tem as seguintes*

propriedades:

$$\alpha(r+s,m) = \alpha(r,m) + \alpha(s,m)$$
$$\alpha(r,m+n) = \alpha(r,m) + \alpha(r,n)$$
$$\alpha(r,\alpha(s,m)) = \alpha(rs,m)$$
$$\alpha(1,m) = m$$

para todos $r,s \in R$ *e* $m,n \in M$.

Para simplificar a notação, se M é um R-módulo com R-ação α em M, escreveremos $\alpha(r,m)$ como rm.

Definição 29 (R-módulo)**.** *Seja R um anel com identidade. Um grupo abeliano aditivo M munido de uma R-ação em M é chamado de R-módulo.*

Definição 30 (Submódulo)**.** *Sejam R um anel com identidade e M um R-módulo. Um subgrupo N de M é chamado de submódulo de M se $rn \in N$ para todo $r \in R$ e $n \in N$.*

Definição 31 (Submódulo gerado por um conjunto)**.** *Se $X \neq \emptyset$ é um subconjunto de um R-módulo M então o submódulo gerado por X é o menor submódulo de M contendo X.*

Mostremos que a definição acima faz sentido. Sejam M um grupo abeliano aditivo, R um anel com identidade e $\alpha : R \times M \to M$ uma R-ação, de forma que M seja um R-módulo. Seja ainda $X \subset M$, com $X \neq \emptyset$. Considere o conjunto:

$$A = \{N \subset M \ \mid \ N \text{ é submódulo de } M \text{ e } X \subset N\}$$

Notemos que M é um submódulo de M e $X \subset M$, donde $A \neq \emptyset$. Seja $L = \bigcap_{N \in A} N \subset M$. Mostremos que L é um submódulo de M que contém X:

- L é um subgrupo de M: Seja $0 \in M$ o elemento neutro da adição em M. Dado $N \in A$, como N é subgrupo de M, temos $0 \in N$, donde $0 \in \bigcap_{N \in A} N = L$ (em particular, $L \neq \emptyset$). Assim, para verificar que L é subgrupo de M, resta apenas mostrar que:

  $$a + b \in L \text{ para todos } a,b \in L$$
  $$-a \in L \text{ para todo } a \in L$$

  Sejam $a,b \in L$. Então, dado $N \in A$, como $L \subset N$, temos $a,b \in N$. Sendo N subgrupo de M, segue que $a+b \in N$ e $-a \in N$. Assim:

  $$a+b, -a \in \bigcap_{N \in A} N = L$$

  donde L é um subgrupo de M.

- L é um submódulo de M: Dados $r \in R$ e $a \in L$, temos que $a \in N$ para todo $N \in A$. Como N é submódulo de M para todo $N \in A$, segue que $ra \in N$ para todo $N \in A$, donde $ra \in \bigcap_{N \in A} N = L$. Assim, como L é um subgrupo de M, segue que L é submódulo de M.

- $X \subset L$: Dado $x \in X \neq \emptyset$, temos que $x \in N$ para todo $N \in A$ (pela definição de A), donde $x \in \bigcap_{N \in A} N = L$. Assim, $X \subset L$.

Note que L é o menor submódulo de M contendo X. De fato, se $K \subset M$ é um submódulo de M e $X \subset K$, então, por definição, temos $K \in A$, donde $L = \bigcap_{N \in A} N \subset K$.

Definição 32 (Submódulo finitamente gerado)**.** *Um R-módulo M é chamado finitamente gerado se M é gerado por um conjunto finito de elementos de M.*

Definição 33 (Módulo quociente)**.** *Seja N um submódulo de um R-módulo M. Então o módulo quociente $\frac{M}{N}$ é o grupo quociente $\frac{M}{N}$ de conjuntos $\{\overline{m} \mid m \in M\}$ munido da R-ação dada por $r(\overline{m}) = \overline{rm}$ para cada $r \in R$ e cada $\overline{m} \in \frac{M}{N}$.*

Definição 34 (Homomorfismo de Módulos)**.** *Sejam M e N R-módulos. Um homomorfismo de módulos de M para N é uma função $\theta : M \to N$ tal que:*

$$\theta(m_1 + m_2) = \theta(m_1) + \theta(m_2)$$
$$\theta(rm_1) = r\theta(m_1)$$

para todos $m_1, m_2 \in M$ e $r \in R$. Um homomorfismo de módulos que é bijetivo é chamado de isomorfismo de módulos. Se $\theta : M \to N$ é um isomorfismo de módulos, dizemos que M e N são módulos isomorfos, e escrevemos $M \simeq N$.

Definiremos agora um módulo Noetheriano de maneira análoga a como fizemos para domínios Noetherianos, e provaremos alguns resultados.

Definição 35 (Módulo Noetheriano)**.** *Seja R um anel com identidade. Um R-módulo M é chamado Noetheriano se toda cadeia ascendente de submódulos de M termina.*

Teorema 40. *Sejam R um anel com identidade, M um R-módulo e N um submódulo de M. Então M é Noetheriano se, e somente se, ambos N e $\frac{M}{N}$ são Noetherianos.*

Demonstração. ($\Rightarrow$) Suponha que M seja Noetheriano. Seja:

$$N_1 \subseteq N_2 \subseteq ...$$

uma cadeia ascendente de submódulos de N. Como N é um submódulo de M esta cadeia é também uma cadeia de submódulos de M. Mas M é Noetheriano, donde esta cadeia termina. Logo N é Noetheriano. Agora, seja:

$$\overline{M_1} \subseteq \overline{M_2} \subseteq ...$$

uma cadeia ascendente de submódulos do módulo quociente $\frac{M}{N}$. Para $i = 1, 2, ...$, seja:

$$M_i = \{m \in M \mid \overline{m} \in \overline{M_i}\}$$

Note que, dados $m \in M_i$ e $r \in R$, temos $\overline{m} \in \overline{M_i} \Rightarrow r\overline{m} = \overline{rm} \in \overline{M_i}$ (pois $\overline{M_i}$ é submódulo de $\frac{M}{N}$) $\Rightarrow rm \in M_i$. Assim, M_i é submódulo de M. Ainda, como $\overline{M_i} \subseteq \overline{M_{i+1}}$, temos $M_i \subseteq M_{i+1}$. Logo:

$$M_1 \subseteq M_2 \subseteq ...$$

é uma cadeia ascendente de submódulos de M. Como M é Noetheriano esta cadeia termina e, consequentemente, a cadeia original também termina. Assim, $\frac{M}{N}$ é Noetheriano.

($\Leftarrow$) Suponha que N e $\frac{M}{N}$ são Noetherianos. Seja:

$$M_1 \subseteq M_2 \subseteq ...$$

uma cadeia ascendente de submódulos de M. Para $i = 1, 2, ...$ seja:

$$\overline{M_i} = \{\overline{m} \mid m \in M_i\}$$

Mostremos que $\overline{M_i}$ é um submódulo de $\frac{M}{N}$. Para isso, basta mostrarmos que:

$$\overline{a}, \overline{b} \in \overline{M_i} \Rightarrow \overline{a+b} = \overline{a} + \overline{b} \in \overline{M_i}$$
$$\overline{a} \in \overline{M_i} \Rightarrow -\overline{a} = \overline{-a} \in \overline{M_i}$$
$$r \in R, \overline{a} \in \overline{M_i} \Rightarrow r\overline{a} = \overline{ra} \in \overline{M_i}$$

Assim:

- $\overline{a}, \overline{b} \in \overline{M_i} \Rightarrow \overline{a+b} = \overline{a} + \overline{b} \in \overline{M_i}$: Pela definição de $\overline{M_i}$, sabemos que $a, b \in M_i$. Assim, $a + b \in M_i$ (pois M_i é um submódulo de M), donde $\overline{a+b} = \overline{a} + \overline{b} \in \overline{M_i}$.
- $\overline{a} \in \overline{M_i} \Rightarrow -\overline{a} = \overline{-a} \in \overline{M_i}$: Pela definição de $\overline{M_i}$, sabemos que $a \in M_i$. Assim, $-a \in M_i$ (pois M_i é submódulo de M), donde $\overline{-a} = -\overline{a} \in \overline{M_i}$.
- $r \in R, \overline{a} \in \overline{M_i} \Rightarrow r\overline{a} = \overline{ra} \in \overline{M_i}$: Pela definição de $\overline{M_i}$, sabemos que $a \in M_i$. Assim, $ra \in M_i$ (pois M_i é submódulo de M), donde $\overline{ra} = r\overline{a} \in \overline{M_i}$.

Logo, $\overline{M_i}$ é submódulo de $\frac{M}{N}$. Ainda, dado $\overline{x} \in \overline{M_i}$, temos $x \in M_i \subset M_{i+1}$, donde $\overline{x} \in \overline{M_{i+1}}$. Portanto, $\overline{M_i} \subset \overline{M_{i+1}}$. Assim:

$$\overline{M_1} \subset \overline{M_2} \subset ...$$

é uma cadeia ascendente de submódulos de $\frac{M}{N}$. Como $\frac{M}{N}$ é um módulo Noetheriano, esta cadeia termina e existe $j_1 \in \mathbb{N}$ tal que:

$$\overline{M_i} \subset \overline{M_{j_1}} \text{ para } i \geq j_1$$

Ainda, $M_i \cap N$ é um submódulo de N e $M_i \cap N \subset M_{i+1} \cap N$, de forma que:

$$M_1 \cap N \subset M_2 \cap N \subset ...$$

é uma cadeia ascendente de submódulos de N. Como N é um módulo Noetheriano, esta cadeia termina e existe $j_2 \in \mathbb{N}$ tal que:

$$M_i \cap N = M_{j_2} \cap N \text{ para } i \geq j_2$$

Definamos $j = \max\{j_1, j_2\}$. Então, para $i \geq j$, temos:

$$\overline{M_i} = \overline{M_{i+1}} \text{ e } M_i \cap N = M_{i+1} \cap N$$

Suponha que a cadeia original $M_1 \subset M_2 \subset ...$ de submódulos de M não termina. Então $M_i \subset M_{i+1}$ para algum $i \geq l$. Assim, existe $m_{i+1} \in M_{i+1} \setminus M_i$. Como $\overline{m_{i+1}} \in \overline{M_{i+1}} = \overline{M_i}$, existem $m_i \in M_i$ e $n \in N$ tais que $m_{i+1} = m_i + n$. Então $m_{i+1} - m_i = n \in N$. Ainda, como $M_i \subset M_{i+1}$, temos $m_{i+1} - m_i \in M_{i+1}$. Então, $m_{i+1} - m_i \in M_{i+1} \cap N = M_i \cap N \subset M_i$, donde $m_{i+1} \in M_i$, o que é um absurdo. Então, a cadeia $M_1 \subset M_2 \subset ...$ deve terminar e M é um módulo Noetheriano. □

Definimos um anel Noetheriano de maneira análoga a definição de um domínio Noetheriano:

Definição 36. *Um anel R é chamado de Noetheriano se toda cadeia ascendente de ideais em R termina.*

Teorema 41. *Se R é um anel Noetheriano, então qualquer R-módulo M finitamente gerado é Noetheriano.*

Demonstração. Seja M um R-módulo finitamente gerado. Então, existem $m_1, m_2, ..., m_n \in M$ tais que:

$$M = Rm_1 + Rm_2 + ... + Rm_n$$

com cada Rm_i sendo um R-módulo. Para cada $k \in \{1, 2, ..., n\}$, definamos o R-módulo M_k como sendo:

$$M_k = Rm_1 + ... + Rm_k$$

de forma que $M_n = M$. Mostremos que cada R-módulo Rm_i é Noetheriano, com $i \in \{1, ..., n\}$. Dado $i \in \{1, ..., n\}$, sejam:

$$N_i = \{r \in R \mid rm_i = 0\}$$

Então:

- $N_i \neq \emptyset$: Como $0 \in R$ é tal que $0m_i = 0$, temos $0 \in N_i$, donde $N_i \neq \emptyset$.

- $a, b \in N_i \Rightarrow a + b \in N_i$: Como $a, b \in N_i$ e R é um anel, temos $a + b \in R$ e:

$$(a + b)\, m_i = am_i + bm_i = 0 + 0 = 0$$

  Logo, $a + b \in N_i$.

- $a \in N_i \Rightarrow -a \in N_i$: Como $a \in N_i$ e R é um anel, temos $-a \in R$ e:

$$0 = (0)\, m_i = (a - a)\, m_i = am_i + (-a)m_i = 0 - am_i = -am_i$$

  Logo, $-a \in N_i$.

- $r \in R, a \in N_i \Rightarrow ra \in N_i$: Como $a \in N_i$ e R é um anel, temos $a \in R$ e $ra \in R$. Assim:

$$(ra)m_i = r(am_i) = r0 = 0$$

  Logo, $ra \in N_i$.

Assim, N_i é um submódulo de R (considerado como um R-módulo). Como os submódulos de R, considerado como um R-módulo, são os ideais de R e R é um anel Noetheriano, segue que R é um módulo Noetheriano. Então, pelo Teorema 40, o módulo quociente $\dfrac{R}{N_i}$ é Noetheriano. Definamos $\theta : Rm_i \to \dfrac{R}{N_i}$ dado por $\theta(rm_i) = \overline{r}$ para todo $r \in R$. Então, dados $r, s \in R$, temos $\theta(rm_i + sm_i) = \theta((r + s)m_i) = \overline{r + s} = \overline{r} + \overline{s} = \theta(rm_i) + \theta(sm_i)$. Ainda, $\theta(s(rm_i)) = \theta((sr)m_i) = \overline{sr} = s\overline{r} = s\theta(rm_i)$. Assim, θ é um homomorfismo de $\dfrac{R}{N_i}$ para Rm_i. Dado $x \in \dfrac{R}{N_i}$, existe $r \in R$ tal que $x = \overline{r}$. Dessa forma, $rm_i \in Rm_i$ e $\theta(rm_i) = \overline{r}$, donde θ é sobrejetora. Da mesma forma, dados $r, s \in R$ tais que $\theta(rm_i) = \theta(sm_i)$, então:

$$\overline{r} = \overline{s} \Rightarrow \overline{r - s} = \overline{0}$$

donde $r - s \in N_i$. Com isso:

$$(r - s)m_i = 0 \Rightarrow rm_i = sm_i$$

e θ é injetora. Assim, θ é um isomorfismo de módulos e $\dfrac{R}{N_i} \simeq Rm_i$. Como $\dfrac{R}{N_i}$ é Noetheriano, temos Rm_i Noetheriano. Em particular, $M_1 = Rm_1$ é Noetheriano. Suponha então que $M_1, ..., M_{k-1}$ é Noetheriano, com $k \in \{2, ..., n\}$. Mostremos que M_k é Noetheriano. Como Rm_k é Noetheriano, temos pelo Teorema 40 que o módulo quociente:

$$\frac{Rm_k}{Rm_k \cap M_{k-1}}$$

é Noetheriano. Então:

$$\frac{M_k}{M_{k-1}} = \frac{M_{k-1} + Rm_k}{M_{k-1}} \simeq \frac{Rm_k}{Rm_k \cap M_{k-1}}$$

é Noetheriano. Pelo Teorema 40, M_k é Noetheriano. Prosseguindo dessa forma, temos que $M_1, ..., M_n$ são módulos Noetherianos, donde $M = M_n$ é um módulo Noetheriano. □

Podemos agora provar o próximo teorema, que será usado em muitos outros resultados.

Teorema 42. *Sejam D e E domínios de integridade com $D \subset E$. Se D é um domínio Noetheriano e E é um D-módulo finitamente gerado então E é um domínio Noetheriano.*

Demonstração. Seja $I_1 \subset I_2 \subset ...$ uma cadeia ascendente de ideais no domínio E. Pelo Teorema 41, como D é um domínio Noetheriano e E é um D-módulo finitamente gerado, temos que E é um D-módulo Noetheriano. Mas cada I_i é um D-submódulo de E, donde a cadeia $I_1 \subset I_2 \subset ...$ deve terminar. Portanto, mostramos que E é um domínio Noetheriano. □

Como consequência deste resultado, temos os seguintes teoremas:

Teorema 43. *Seja $m \in \mathbb{Z}$ livre de quadrados. Então $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ é um domínio Noetheriano*

Demonstração. Tomemos $D = \mathbb{Z}$ e $E = \mathbb{Z} + \mathbb{Z}\sqrt{m}$ no Teorema 42. Como $\mathbb{Z}$ é um domínio Noetheriano e $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é um $\mathbb{Z}$-módulo finitamente gerado, o resultado segue. □

Em particular, pelo Teorema 37, vemos que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ é um domínio de fatoração para todo $m \in \mathbb{Z}$ livre de quadrados. Com isso, sabemos que $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$ é um domínio de fatoração. Note ainda que $2, 3, 1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ são irredutíveis em $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$. De fato, sejam $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Então:

- $\left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = 2$: Neste caso, usando a função ϕ_{-5}, temos:

  $$4 = (a^2 + 5b^2)(c^2 + 5d^2)$$

  donde $a^2+5b^2 \mid 4$. Caso $a^2+5b^2 = 1$, temos $a+b\sqrt{-5} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{-5})$. Analogamente, caso $a^2 + 5b^2 = 4$, então $c^2 + 5d^2 = 1$ e $c + d\sqrt{-5} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$. Nos resta então analisar o caso $a^2 + 5b^2 = 2$. Neste caso, se $b \neq 0$, então $a^2 + 5b^2 \geq 5b^2 \geq 5 > 2$. Logo, $b = 0$ e $a^2 = 2$, donde $a = \pm\sqrt{2} \notin \mathbb{Z}$, o que é um absurdo. Portanto, 2 é irredutível em $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

- $\left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = 3$: Este caso é análogo ao anterior.

- $\left(a + b\sqrt{-5}\right)\left(c + d\sqrt{-5}\right) = 1 + \sqrt{-5}$ ou $1 - \sqrt{-5}$: Neste caso, usando a função ϕ_{-5}, temos:

  $$6 = 1^2 + 5((\pm 1)^2) = (a^2 + 5b^2)(c^2 + 5d^2)$$

  donde $a^2+5b^2 \mid 6$. Caso $a^2+5b^2 = 1$, temos $a+b\sqrt{-5} \in U(\mathbb{Z}+\mathbb{Z}\sqrt{-5})$. Analogamente, caso $a^2 + 5b^2 = 6$, então $c^2 + 5d^2 = 1$ e $c + d\sqrt{-5} \in U(\mathbb{Z} + \mathbb{Z}\sqrt{-5})$. Nos resta então analisar os casos $a^2 + 5b^2 = 2$ ou $a^2 + 5b^2 = 3$. Pelos itens anteriores, sabemos que ambos os casos são impossíveis. Portanto, $1 + \sqrt{-5}$ e $1 - \sqrt{-5}$ são irredutíveis em $\mathbb{Z} + \mathbb{Z}\sqrt{-5}$.

Com isso, $2, 3, 1+\sqrt{-5}$ e $1-\sqrt{-5}$ são irredutíveis em $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$, mas:

$$6 = 2 \times 3 = \left(1+\sqrt{-5}\right) \times \left(1-\sqrt{-5}\right)$$

Como $U(\mathbb{Z}+\mathbb{Z}\sqrt{-5}) = \{-1, 1\}$ e quaisquer dois elementos dentre $2, 3, 1+\sqrt{-5}$ e $1-\sqrt{-5}$ são distintos e não são opostos, 6 não tem fatoração única. Logo, $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ é um domínio de fatoração que não é um domínio de fatoração única. Ou seja, nem todo domínio de fatoração é um domínio de fatoração única, como havíamos mencionado.

Por fim, tomando $m \in \mathbb{Z}$ livre de quadrados com $m \equiv 1 \pmod 4$ e fazendo $D = \mathbb{Z}$ e $E = \mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ no Teorema 42, obtemos o seguinte resultado, análogo ao teorema anterior:

Teorema 44. *Seja $m \in \mathbb{Z}$ livre de quadrados com $m \equiv 1 \pmod 4$. Então $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ é um domínio Noetheriano.*

Ainda, por consequência do Teorema 37, temos que, se $m \in \mathbb{Z}$, m é livre de quadrados e $m \equiv 1 \pmod 4$, então $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ é um domínio de fatoração.

2.8 DECOMPOSIÇÃO DE INTEIROS EM PARTE LIVRE DE QUADRADOS

Como última seção deste capítulo de teoria introdutória, apresentaremos um resultado de teoria elementar dos números, o qual será utilizado em alguns resultados ao longo do texto e no estudo de certas equações diofantinas, no último capítulo.

Proposição 14 (Decomposição em parte livre de quadrados)**.** *Dado $m \in \mathbb{Z} \setminus \{0\}$, existem únicos $d, l \in \mathbb{N}^*$ e $u \in \{-1, 1\}$, com l livre de quadrados, tais que:*

$$m = ud^2l$$

Demonstração. • **Existência**: Primeiramente, suponha $m > 0$. Se $m = 1$, temos que $u = d = l = 1$ satisfaz $m = 1 = ud^2l$, com l livre de quadrados. Se $m > 1$, sabemos pelo Algoritmo de Euclides que existe $n \in \mathbb{N}$, $p_1, ..., p_n \in \mathbb{N}$ primos e $\alpha_1, ..., \alpha_n \in \mathbb{N}$ tais que $m = \prod_{i=1}^{n} p_i^{\alpha_i}$. Sejam $d = \prod_{i=1}^{n} p_i^{\left\lfloor \frac{\alpha_i}{2} \right\rfloor}$, $l = \prod_{i=1}^{n} p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor}$ e $u = 1$. Temos:

1. $d, l \in \mathbb{N}$: Dado $i \in \{1, ..., n\}$, sabemos que $\alpha_i \in \mathbb{N} \Rightarrow \alpha_i \geq 0 \Rightarrow \frac{\alpha_i}{2} \geq 0 \Rightarrow \left\lfloor \frac{\alpha_i}{2} \right\rfloor \geq 0$ e $\left\lfloor \frac{\alpha_i}{2} \right\rfloor \in \mathbb{Z} \Rightarrow \left\lfloor \frac{\alpha_i}{2} \right\rfloor \in \mathbb{N} \Rightarrow p_i^{\left\lfloor \frac{\alpha_i}{2} \right\rfloor} \in \mathbb{N}^*$ (uma vez que $p_i \in \mathbb{N}^*$). Como isso vale para todo $i \in \{1, ..., n\}$, temos $\prod_{i=1}^{n} p_i^{\left\lfloor \frac{\alpha_i}{2} \right\rfloor} = d \in \mathbb{N}^*$. Ainda, dado $i \in \{1, ..., n\}$, temos duas possibilidades:

– Caso $\alpha_i \equiv 0 \pmod 2$: Neste caso, temos $\alpha_i = 2\beta_i$, com $\beta_i \in \mathbb{N}^*$. Assim, $\frac{\alpha_i}{2} = \beta_i \Rightarrow \left\lfloor \frac{\alpha_i}{2} \right\rfloor = \lfloor \beta_i \rfloor = \beta_i \in \mathbb{N}^*$. Dessa forma:

$$\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor = 2\beta_i - 2\beta_i = 0 \in \mathbb{N}$$

Logo, $p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor} \in \mathbb{N}^*$.

– Caso $\alpha_i \equiv 1 \pmod 2$: Neste caso, temos $\alpha_i = 2\beta_i + 1$, com $\beta_i \in \mathbb{N}^*$. Assim, $\frac{\alpha_i}{2} = \beta_i + \frac{1}{2} \Rightarrow \left\lfloor \frac{\alpha_i}{2} \right\rfloor = \left\lfloor \beta_i + \frac{1}{2} \right\rfloor = \beta_i \in \mathbb{N}^*$. Dessa forma:

$$\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor = 2\beta_i + 1 - 2\beta_i = 1 \in \mathbb{N}$$

Logo, $p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor} \in \mathbb{N}^*$.

Portanto, $\prod_{i=1}^{n} p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor} = l \in \mathbb{N}^*$.

2. l é livre de quadrados: Basta notar que $l = \prod_{i=1}^{n} p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor}$ é uma decomposição em primos (e, portanto, a única decomposição em primos) de l. Assim, para que l seja livre de quadrados, basta que $\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor \in \{0, 1\}$ para todo $i \in \{1, ..., n\}$, o que foi verificado no item anterior.

3. $m = ud^2l$: Este fato segue por verificação imediata:

$$ud^2l = 1 \times \left(\prod_{i=1}^{n} p_i^{\left\lfloor \frac{\alpha_i}{2} \right\rfloor} \right)^2 \times \prod_{i=1}^{n} p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor} = \left(\prod_{i=1}^{n} p_i^{\left\lfloor \frac{\alpha_i}{2} \right\rfloor} \right)^2 \times \prod_{i=1}^{n} p_i^{\alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor}$$

$$= \prod_{i=1}^{n} p_i^{2\left\lfloor \frac{\alpha_i}{2} \right\rfloor + \alpha_i - 2\left\lfloor \frac{\alpha_i}{2} \right\rfloor} = \prod_{i=1}^{n} p_i^{\alpha_i} = m$$

Note que, para todos os casos em que $m > 0$, tomamos $u = 1$. Assim, para o caso $m < 0$, temos $-m > 0$, donde existem $l, d \in \mathbb{N}^*$, com l livre de quadrados, tais que $-m = d^2l \Rightarrow m = (-1)\, d^2l$. Portanto, para todo $m \in \mathbb{Z} \setminus \{0\}$, existem $d, l \in \mathbb{N}^*$, com l livre de quadrados, e $u \in \{-1, 1\}$, tais que $m = ud^2l$.

- **Unicidade**: Primeiramente, suponha $m > 0$. Se $m = 1$, seja $1 = ud^2l$ uma decomposição em parte livre de quadrados de 1. Note que $d, l \in \mathbb{N}^*$ implica em $d^2, l \geq 1 \Rightarrow d^2l \geq 1 > 0$. Assim, se tivéssemos $u = -1$, seguiria que $1 = ud^2l < 0$, o que é um absurdo. Logo, $u = 1$, donde $d^2l = 1$. Logo, $d^2, l \mid 1$ e $l, d^2 \in \mathbb{N}^* \Rightarrow l = d^2 = 1$ e $d \in \mathbb{N}^*$, donde $d = 1$. Portanto, a única decomposição em parte livre de quadrados de 1 é, de fato, $u = l = d = 1$. Se $m \neq 1$, sejam $m = vD^2L = ud^2l$

duas decomposições em parte livre de quadrados de m. Como $D, L, d, l \in \mathbb{N}^*$, temos $D^2L, d^2l > 0$. Sendo $m > 0$, devemos então ter $u = v = 1$. Assim, $m = D^2L = d^2l$. Sejam $m = \prod_{i=1}^{n} p_i^{\alpha_i}$, $d = \prod_{i=1}^{n} p_i^{\beta_i}$, $l = \prod_{i=1}^{n} p_i^{\theta_i}$, $D = \prod_{i=1}^{n} p_i^{\omega_i}$ e $L = \prod_{i=1}^{n} p_i^{\zeta_i}$ as fatorações em primos de m, l, d, D e L. Temos $m = \prod_{i=1}^{n} p_i^{\alpha_i} = \prod_{i=1}^{n} p_i^{2\omega_i+\zeta_i} = \prod_{i=1}^{n} p_i^{2\beta_i+\theta_i}$. Dado $i \in \{1, ..., n\}$, temos duas possibilidades:

- Caso $\alpha_i \equiv 0 \pmod 2$: Neste caso, afirmo que $\theta_i = \zeta_i = 0$. Sabemos que $\alpha_i = 2\beta_i + \theta_i \Rightarrow \theta_i = \alpha_i - 2\beta_i \equiv \alpha_i \equiv 0 \pmod 2$. Analogamente, $\alpha_i = 2\omega_i + \zeta_i \Rightarrow \zeta_i = \alpha_i - 2\omega_i \equiv \alpha_i \equiv 0 \pmod 2$. Como L, l são livres de quadrados, devemos ter $\zeta_i, \theta_i \in \{0, 1\}$. Assim, $\theta_i = \zeta_i = 0$.
- Caso $\alpha_i \equiv 1 \pmod 2$: Neste caso, afirmo que $\theta_i = \zeta_i = 1$. Sabemos que $\alpha_i = 2\beta_i + \theta_i \Rightarrow \theta_i = \alpha_i - 2\beta_i \equiv \alpha_i \equiv 1 \pmod 2$. Analogamente, $\alpha_i = 2\omega_i + \zeta_i \Rightarrow \zeta_i = \alpha_i - 2\omega_i \equiv \alpha_i \equiv 1 \pmod 2$. Como L, l são livres de quadrados, devemos ter $\zeta_i, \theta_i \in \{0, 1\}$. Assim, $\theta_i = \zeta_i = 1$.

Logo, $\theta_i = \zeta_i$ para todo $i \in \{1, ..., n\}$, donde temos $L = \prod_{i=1}^{n} p_i^{\zeta_i} = \prod_{i=1}^{n} p_i^{\theta_i} = l$. Assim, de $D^2L = d^2l$ e de $L, l \in \mathbb{N}^*$ (isto é, de $L, l \neq 0$), segue que $D^2 = d^2 \Rightarrow d = \pm D$. Como ambos $d, D \in \mathbb{N}^*$, temos $d = D$. Portanto, m possui única decomposição em parte livre de quadrados.

Suponha agora $m < 0$. Seja $m = ud^2l$ uma decomposição em parte livre de quadrados. Como $d, l \in \mathbb{N}^*$, temos $d^2l \in \mathbb{N}^*$, donde $d^2l > 0$. Se tivéssemos $u = 1$, seguiria que $m = ud^2l > 0$, o que é um absurdo. Assim, $u = -1$. Dessa forma, $m = -d^2l$. Seja $m = vD^2L$ outra decomposição em parte livre de quadrados. Como acabamos de mostrar, devemos ter $v = -1$, donde $m = -d^2l = -D^2L \Rightarrow -m = d^2l = D^2L$. Note que $-m > 0$, $d, l, D, L \in \mathbb{N}^*$ e l, L são livres de quadrados. Por definição, segue que d^2l e D^2L são decomposições em parte livre de quadrados de $-m > 0$. Pelo que já mostramos, isso implica em $d = D$ e $l = L$. Portanto, m possui única decomposição em parte livre de quadrados.

□

Pela demonstração anterior, mostramos não apenas que $m \in \mathbb{Z} \setminus \{0\}$ possui decomposição única em parte livre de quadrados, mas também que $u = sig(m)$, em que $sig : \mathbb{Z} \setminus \{0\} \to \{-1, 1\}$ é a função sinal, dada por $sig(z) = 1$ se $z > 0$ e $sig(z) = -1$ caso $z < 0$.

3 ELEMENTOS INTEIROS SOBRE UM DOMÍNIO

No capítulo anterior, estudamos diversos tipos de domínios e suas propriedades. Nos resta ainda estudar mais um tipo de domínio, os domínios de Dedekind, o qual será o último tópico apresentado antes das equações diofantinas, e que terá papel fundamental na análise destas. Por isso, neste capítulo e nos próximos, estudaremos a teoria necessária para definirmos e analisarmos os domínios de Dedekind. Em particular, neste capítulo, estudaremos os elementos inteiros sobre um domínio e os resultados associados a estes elementos, que servirão de base para os próximos capítulos.

3.1 ELEMENTOS INTEIROS SOBRE UM DOMÍNIO

Definição 37 (Elementos inteiros sobre um domínio)**.** *Sejam A e B domínios de integridade com $A \subseteq B$. O elemento $b \in B$ é dito inteiro sobre A se ele satisfaz uma equação polinomial:*

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0,$$

em que $a_0, a_1, ..., a_{n-1} \in A$.

Em outras palavras, um elemento $b \in B$ é inteiro sobre A quando existe um polinômio mônico $p(x) \in A[x]$ tal que $p(b) = 0$.

Vale notar que, se $a \in A$, temos que a satisfaz a equação polinomial $x - a = 0$ e $x - a \in A[x]$. Como, na definição de elemento inteiro, exigimos que $A \subseteq B$, segue que um elemento de A é sempre inteiro sobre A, qualquer que seja o domínio B.

Definição 38 (Inteiro algébrico)**.** *Um número complexo que é inteiro sobre $\mathbb{Z}$ é chamado de inteiro algébrico.*

Definição 39 (Elemento algébrico sobre um corpo)**.** *Sejam A e B domínios de integridade com $A \subseteq B$. Suponha que A é um corpo e $b \in B$ é inteiro sobre A. Então b é dito algébrico sobre A.*

Definição 40 (Número algébrico)**.** *Um número complexo que é algébrico sobre $\mathbb{Q}$ é dito um número algébrico.*

Definição 41 (Domínio inteiro sobre um subdomínio)**.** *Sejam $A \subseteq B$ domínios de integridade. Se todo $b \in B$ é inteiro sobre A dizemos que B é inteiro sobre A.*

Provaremos agora algumas propriedades dos elementos inteiros sobre um domínio.

Teorema 45. *Sejam $A \subseteq B \subseteq C$ uma torre de domínios de integridade. Se $c \in C$ é inteiro sobre A então c é inteiro sobre B.*

Demonstração. Como $c \in C$ é inteiro sobre A então existem $a_0, a_1, ..., a_{n-1} \in A$ tal que:

$$c^n + a_{n-1}c^{n-1} + ... + a_1c + a_0 = 0$$

Como $A \subseteq B$, $a_0, a_1, ..., a_{n-1} \in B$ e assim c é inteiro sobre B. □

Teorema 46. *Sejam $A \subseteq B \subseteq C$ uma torre de domínios de integridade. Se C é inteiro sobre A então C é inteiro sobre B.*

Demonstração. Seja $c \in C$. Como C é inteiro sobre A, c é inteiro sobre A. Assim, c é inteiro sobre B para todo $c \in C$, donde C é inteiro sobre B. □

Usaremos agora da teoria referente a seção de módulos no capítulo anterior para mostrar alguns resultados. Antes, entretanto, definiremos um conjunto:

Definição 42. *Sejam A e B domínios de integridade com $A \subset B$. Definimos o domínio de integridade $A[b]$ como $A[b] = \{p(b) \mid p(x) \in A[x]\}$. Como $A \subset A[b] \subset B$, para mostrar que $A[b]$ é domínio de integridade, basta mostrarmos que ele é fechado para a soma e o para o produto e que o inverso aditivo de todo elemento de $A[b]$ está em $A[b]$. Assim, sejam $a, c \in A[b]$. Então existem $p(x), q(x) \in A[x]$ tais que $a = p(b)$ e $c = q(b)$. Ainda, como $p(x) + q(x), p(x)q(x), -p(x) \in A[x]$, segue que:*

$$a + c = p(b) + q(b) \in A[b], \ -a = -p(b) \in A[b] \text{ e } ac = p(b)q(b) \in A[b]$$

donde $A[b]$ é, de fato, um domínio de integridade.

Teorema 47. *Sejam A e B um domínio de integridade com $A \subseteq B$ e $b \in B$. Então b é inteiro sobre A se, e somente se, $A[b]$ é um A-módulo finitamente gerado.*

Demonstração. ($\Rightarrow$) Suponha que b é inteiro sobre A. Então existem $a_0, a_1, ..., a_{n-1} \in A$ tais que:

$$b^n - a_{n-1}b^{n-1} - a_{n-2}b^{n-2} - ... - a_1b - a_0 = 0$$

Então:

$$b^n = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + ... + a_1b + a_0 \in Ab^{n-1} + Ab^{n-2} + ... + Ab + A$$

Ainda:

$$\begin{aligned} b^{n+1} &= a_{n-1}b^n + a_{n-2}b^{n-1} + ... + a_1b^2 + a_0b \\ &\in Ab^n + Ab^{n-1} + ... + Ab^2 + Ab \\ &\subseteq Ab^{n-1} + ... + Ab + A \end{aligned}$$

Por indução, vemos que:

$$b^k \in Ab^{n-1} + ... + Ab + A$$

para todos os inteiros k não negativos. Isso mostra que o domínio de integridade $A[b]$ de polinômios em b com coeficientes em A é um A-módulo finitamente gerado.

($\Leftarrow$) Por outro lado, suponha que $A[b]$ é um A-módulo finitamente gerado. Então existem $u_1, u_2, ..., u_n \in A[b]$ tais que:

$$A[b] = Au_1 + ... + Au_n$$

Sabemos que $u_1, ..., u_n$ não são todos zero. Então, como cada $u_i \in A[b]$, segue que $bu_i \in A[b]$, para cada $i = 1, 2, ..., n$. Com isso, existem $a_{ij} \in A\,(i, j = 1, 2, ..., n)$ tais que:

$$\begin{cases} bu_1 = a_{11}u_1 + ... + a_{1n}u_n \\ \qquad\qquad ... \\ bu_n = a_{n1}u_1 + ... + a_{nn}u_n \end{cases}$$

Assim, o sistema de n equações nas n variáveis $x_1, ..., x_n$:

$$\begin{cases} (b - a_{11})\,x_1 - a_{12}x_2 - ... - a_{1n}x_n = 0 \\ -a_{21}x_1 + (b - a_{22})\,x_2 - ... - a_{2n}x_n = 0 \\ \qquad\qquad\qquad ... \\ -a_{n1}x_1 - a_{n2}x_2 - ... + (b - a_{nn})\,x_n = 0 \end{cases}$$

tem uma solução não trivial $(x_1, x_2, ..., x_n) = (u_1, u_2, ..., u_n)$ no domínio de integridade $A[b]$ e, consequentemente, em seu corpo quociente. Isso ocorre se, e somente se, o determinante da matriz dos coeficientes do sistema é zero. Assim:

$$\begin{vmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{12} & b - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & b - a_n n \end{vmatrix} = 0$$

Calculando este determinante, obtemos a equação:

$$b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0 = 0$$

em que $a_0, a_1, ..., a_{n-1} \in A$. Logo, b é inteiro sobre A. □

Teorema 48. *Sejam A e B domínios de integridade com $A \subseteq B$ e $b \in B$. Se existe um domínio de integridade C tal que $A[b] \subseteq C \subseteq B$ e C é um A-módulo finitamente gerado então b é inteiro sobre A e $A[b]$ é um A-módulo finitamente gerado.*

Demonstração. Como C é um A-módulo finitamente gerado, existem $c_1, ..., c_n \in C$ tais que $C = Ac_1 + ... + Ac_n$. Ainda, temos $c_1, ..., c_n$ não todos simultaneamente nulos. Então $b \in A[b] \subseteq C$ tal que $b \in C$. Mas C é domínio de integridade, donde $bc_1, ..., bc_n \in C$. Então existem $a_{ij} \in A\,(i, j = 1, ..., n)$ tais que:

$$\begin{cases} bc_1 = a_{11}c_1 + ... + a_{1n}c_n \\ \qquad\qquad ... \\ bc_n = a_{n1}c_1 + ... + a_{nn}c_n \end{cases}$$

Assim, o sistema homogêneo de n equações nas n variáveis $x_1, ..., x_n$ dado por:

$$\begin{cases} (b - a_{11})\, x_1 - a_{12}x_2 - ... - a_{1n}x_n = 0 \\ -a_{21}x_1 + (b - a_{22})\, x_2 - ... - a_{2n}x_n = 0 \\ \qquad\qquad\qquad ... \\ -a_{n1}x_1 - a_{n2}x_2 - ... + (b - a_{nn})\, x_n = 0 \end{cases}$$

tem uma solução não trivial $(x_1, ..., x_n) = (c_1, ..., c_n)$ no domínio de integridade C e consequentemente em seu corpo quociente. Portanto, o determinante da matriz dos coeficientes do sistema é zero. Isto é:

$$\begin{vmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{12} & b - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & b - a_n n \end{vmatrix} = 0$$

Expandindo este determinante, obtemos a equação:

$$b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0 = 0$$

em que $a_0, a_1, ..., a_{n-1} \in A$. Assim, b é inteiro sobre A e, pelo Teorema 47, $A[b]$ é um A-módulo finitamente gerado. □

Corolário 3. *Sejam A e B domínios de integridade com $A \subseteq B$ e B um A-módulo finitamente gerado. Então B é inteiro sobre A.*

Demonstração. Sejam $b \in B$, B um A-módulo finitamente gerado tal que $A[b] \subseteq B$. Pelo teorema anterior, temos b inteiro sobre A. Como $b \in B$ foi tomado arbitrariamente, segue que B é inteiro sobre A. □

Teorema 49. *Sejam $A \subseteq B \subseteq C$ uma torre de domínios de integridade. Se B é um A-módulo finitamente gerado e C é um B-módulo finitamente gerado então C é um A-módulo finitamente gerado.*

Demonstração. Como B é um A-módulo finitamente gerado existem $b_1, ..., b_m \in B$ tais que:

$$B = Ab_1 + ... + Ab_m$$

Como C é um B-módulo finitamente gerado, existem $c_1, ..., c_n \in C$ tais que:

$$C = Bc_1 + ... + Bc_n$$

Seja $c \in C$. Então:

$$c = \sum_{j=1}^{n} x_j c_j$$

em que $x_1, ..., x_n \in B$. Ainda, para $j = 1, ..., n$ temos:

$$x_j = \sum_{i=1}^{m} a_{ij} b_i$$

em que $a_{11}, ..., a_{1n}, a_{21}, ..., a_{mn} \in A$. Então:

$$c = \sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij} b_i c_j$$

Logo:

$$C = Ab_1c_1 + ... + Ab_mc_n$$

é um A-módulo finitamente gerado. □

Usaremos dos teoremas anteriores para provar diversos resultados ao longo do restante do capítulo. Em particular, os usaremos para mostrar o próximo teorema, que revela propriedades algébricas sobre os elementos inteiros sobre um domínio e que tem consequências importantes.

Teorema 50. *Sejam A e B domínios de integridade com $A \subseteq B$ e $b_1, b_2 \in B$ inteiros sobre A. Então $b_1 + b_2, b_1 - b_2$ e $b_1 b_2$ são inteiros sobre A.*

Demonstração. Como b_1 é inteiro sobre A, pelo Teorema 47 temos que $A[b_1]$ é um A-módulo finitamente gerado. Ainda, b_2 é inteiro sobre A donde, pelo Teorema 45, segue que b_2 é inteiro sobre $A[b_1]$. Assim, pelo Teorema 47, $(A[b_1])[b_2] = A[b_1, b_2]$ é um $A[b_1]$-módulo finitamente gerado. Pelo teorema anterior, segue que $A[b_1, b_2]$ é um A-módulo finitamente gerado. Seja $\lambda \in \{b_1 + b_2, b_1 - b_2, b_1 b_2\}$. Temos:

$$A \subseteq A[\lambda] \subseteq A[b_1, b_2] \subseteq B$$

em que o domínio de integridade $A[b_1, b_2]$ é um A-módulo finitamente gerado. Pelo Teorema 48, segue que λ é inteiro sobre A. □

Pelo resultado anterior, vemos que o conjunto dos elementos de B que são inteiros sobre A é fechado para a adição e para o produto. Ainda, como $0 \in B$ é inteiro sobre A, temos que $b \in B$ inteiro sobre A implica em $-b = 0 - b$ inteiro sobre A, donde todo elemento neste conjunto possui inverso aditivo. Como as operações neste conjunto são herdadas de B (domínio de integridade) e $1 \in A \cap B$, donde 1 é inteiro sobre A, segue que o conjunto dos elementos de B que são inteiros sobre A é um domínio de integridade. Com isso, temos:

Corolário 4. *Sejam A e B domínios de integridade com $A \subseteq B$. Então o conjunto de todos os elementos de B que são inteiros sobre A é um subdomínio de B contendo A.*

Em particular, tomando $A = \mathbb{Z}$ e $B = \mathbb{C}$ no corolário anterior, segue que:

Corolário 5. *O conjunto dos inteiros algébricos é um domínio de integridade.*

Denotaremos por Ω o conjunto dos inteiros algébricos.

Teorema 51. *Sejam A e B domínios de integridade com $A \subseteq B$ e $b_1, ..., b_n \in B$ inteiros sobre A. Então $A[b_1, ..., b_n]$ é um A-módulo finitamente gerado.*

Demonstração. Provaremos por indução sobre n. Se $b_1 \in B$ é inteiro sobre A então $A[b_1]$ é um A-módulo finitamente gerado pelo Teorema 47, donde o resultado segue para $n = 1$.

Suponha que $A[b_1, ..., b_{n-1}]$ $(n \geq 2)$ é um A-módulo finitamente gerado, em que $b_1, ..., b_{n-1} \in B$ são inteiros sobre A. Seja $b_n \in B$ inteiro sobre A. Então, pelo Teorema 45, b_n é inteiro sobre $A[b_1, ..., b_{n-1}]$. Assim, pelo Teorema 47, $(A[b_1, ..., b_{n-1}])[b_n] = A[b_1, ..., b_n]$ é um A-módulo finitamente gerado. Pelo princípio de indução, o resultado segue. □

Teorema 52. *Sejam A e B domínios de integridade com $A \subseteq B$. Se cada um dos $b_1, ..., b_n \in B$ for inteiro sobre A então $A[b_1, ..., b_n]$ é inteiro sobre A.*

Demonstração. Provaremos por indução sobre n. Suponha que $b_1 \in B$ é inteiro sobre A. Então, pelo Teorema 50, sabemos que $a_0 + a_1 b_1 + ... + a_n b_1^n$ é inteiro sobre A para todo $a_0, a_1, ..., a_n \in A$. Isso mostra que $A[b_1]$ é inteiro sobre A.

Suponha agora que $b_1, ..., b_{n-1} \in B$ são inteiros sobre A e suponha que $A[b_1, ..., b_{n-1}]$ é inteiro sobre A. Sejam $b_n \in B$ inteiro sobre A e $f \in A[b_1, ..., b_n]$. Então:

$$f = f_0 + f_1 b_n + ... + f_m b_n^m$$

em que $f_0, f_1, ..., f_m \in A[b_1, ..., b_{n-1}]$. Pela hipótese de indução sabemos que $f_0, f_1, ..., f_m$ são inteiros sobre A. Então, como b_n é inteiro sobre A, deduzimos pelo Teorema 50 que $f_0 + f_1 b_n + ... + f_m b_n^m = f$ é inteiro sobre A. Portanto todo elemento $f \in A[b_1, ..., b_n]$ é inteiro sobre A, donde temos $A[b_1, ..., b_n]$ inteiro sobre A. Por indução, o resultado segue. □

Teorema 53. *Sejam $A \subseteq B \subseteq C$ uma torre de domínios de integridade. Se B é inteiro sobre A e $c \in C$ é inteiro sobre B então c é inteiro sobre A.*

Demonstração. Como $c \in C$ é inteiro sobre B, existem $b_0, b_1, ..., b_{n-1} \in B$ tais que:

$$c^n + b_{n-1} c^{n-1} + ... + b_1 c + b_0 = 0$$

Isso mostra que c é inteiro sobre $A[b_0, b_1, ..., b_{n-1}]$. Como B é inteiro sobre A, segue que cada b_i é inteiro sobre A. Assim, pelo Teorema 51, $A[b_0, b_1, ..., b_{n-1}]$ é um A-módulo finitamente gerado. Como c é inteiro sobre $A[b_0, b_1, ..., b_{n-1}]$, pelo Teorema 47 temos que $(A[b_0, b_1, ..., b_{n-1}])[c] = A[b_0, b_1, ..., b_{n-1}, c]$ é um A-módulo finitamente gerado. Portanto, pelo Teorema 48, segue que c é inteiro sobre A. □

Com esses resultados, segue que um domínio ser inteiro sobre outro é uma relação transitiva.

Teorema 54. *Sejam $A \subseteq B \subseteq C$ uma torre de domínios de integridade. Se C é inteiro sobre B e B é inteiro sobre A então C é inteiro sobre A.*

3.2 FECHO INTEIRO

Sejam A e B domínios de integridade com $A \subseteq B$. No Corolário 4 mostramos que o conjunto de todos os elementos de B que são inteiros sobre A é um subdomínio de B contendo A. Veremos agora algumas das propriedades deste domínio.

Definição 43 (Fecho inteiro)**.** *Sejam A e B domínios de integridade com $A \subseteq B$. O fecho inteiro de A em B é o subdomínio de B consistindo de todos os elementos de B que são inteiros sobre A. O fecho inteiro de A em B é denotado por A^B.*

Pelo Corolário 4, temos:

Proposição 15. *Sejam A e B domínios de integridade com $A \subseteq B$. Então o fecho inteiro A^B de A em B é um domínio de integridade satisfazendo:*

$$A \subseteq A^B \subseteq B$$

Teorema 55. *Sejam D um domínio de fatoração única e F o corpo quociente de D. Então $c \in F$ é inteiro sobre D se, e somente se, $c \in D$.*

Demonstração. ($\Leftarrow$) Se $c \in D$ então c satisfaz a equação $x - c = 0$ e, portanto, c é inteiro sobre D.

($\Rightarrow$) Suponha que $c \in F$ é inteiro sobre D. Então c satisfaz uma equação polinomial:

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$$

em que $a_0, a_1, ..., a_{n-1} \in D$. Como $c \in F$ podemos expressar c na forma $\frac{r}{s}$, com $r, s \in D$, $s \neq 0$ e $(r, s) = 1$. Assim:

$$r^n + a_{n-1}r^{n-1}s + ... + a_1rs^{n-1} + a_0s^n = 0$$

Se $s \notin U(D)$ então existe $p \in D$ primo tal que $p \mid s$. Pela equação anterior, vemos que $p \mid -a_{n-1}r^{n-1}s - ... - a_1rs^{n-1} - a_0s^n = r^n$. Consequentemente, temos $p \mid r$. Isso contradiz $(r, s) = 1$. Portanto, $s \in U(D)$ e $c = rs^{-1} \in D$. □

Como consequência do teorema anterior, temos o seguinte resultado:

Proposição 16. $\mathbb{Q} \cap \Omega = \mathbb{Z}$.

Demonstração. Sabemos que $\mathbb{Z}$ é um domínio de fatoração única. Pelo Teorema 55, fazendo $D = \mathbb{Z}$, temos $F = \mathbb{Q}$ e segue que $c \in \mathbb{Q} \cap \Omega$ se, e somente se, $c \in \mathbb{Z}$. Portanto, $\mathbb{Q} \cap \Omega = \mathbb{Z}$. □

O Teorema 55 nos mostra que os domínios de fatoração única D satisfazem a propriedade $D^F = D$, sendo F o corpo quociente de D. Tal fato nos leva à seguinte definição:

Definição 44 (Domínio inteiramente fechado)**.** *Um domínio de integridade D é dito inteiramente fechado se os únicos elementos de seu corpo quociente que são inteiros sobre D são os elementos de D.*

Pelo Teorema 55, temos:

Proposição 17. *Seja D um domínio de fatoração única. Então D é inteiramente fechado.*

Por fim, temos um resultado que nos revela a forma de um número algébrico.

Teorema 56. *Todo número algébrico é da forma $\frac{a}{b}$, em que a é um inteiro algébrico e $b \in \mathbb{Z} \setminus \{0\}$.*

Demonstração. Seja c um número algébrico. Então existem $a_0, a_1, ..., a_{n-1} \in \mathbb{Q}$ tais que:

$$c^n + a_{n-1}c^{n-1} + ... + a_1 c + a_0 = 0$$

Seja b o mmc dos denominadores de $a_0, a_1, ..., a_{n-1}$. Então $b \in \mathbb{N}$ e $ba_i \in \mathbb{Z}$ para $i \in \{0, 1, ..., n-1\}$. Pela equação acima, temos:

$$(bc)^n + (ba_{n-1})(bc)^{n-1} + ... + \left(b^{n-1}a_1\right)(bc) + (b^n a_0) = 0$$

Portanto, bc é a raiz de um polinômio mônico em $\mathbb{Z}$. Assim, bc é um inteiro algébrico a. Logo, $c = \frac{a}{b}$, com $a \in \Omega$ e $b \in \mathbb{Z} \setminus \{0\}$. □

4 EXTENSÕES ALGÉBRICAS DE UM CORPO

Estudaremos agora extensões de corpos, polinômios mínimos e conjugados de um elemento. Um dos principais objetivos deste estudo é conseguir encontrar uma forma mais simples de representar os elementos da extensão de um corpo em função dos elementos do corpo original e dos elementos adjuntados a esse corpo. Através disso, conseguiremos explicitar a forma dos inteiros algébricos em certas extensões de corpos, os quais possuem propriedades importantes que se conectam com alguns dos domínios estudados, como $\mathbb{Z}+\mathbb{Z}\sqrt{n}$ e $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$.

4.1 POLINÔMIO MÍNIMO DE UM ELEMENTO ALGÉBRICO SOBRE UM CORPO

Sejam $K \subset \mathbb{C}$ um subcorpo e $\alpha \in \mathbb{C}$ algébrico sobre K. Como α é algébrico sobre K, existe $q(x) \in K[x] \setminus \{0(x)\}$ tal que $q(\alpha) = 0$. Assim, considere o conjunto $I_K(\alpha) = \{f(x) \in K[x] \mid f(\alpha) = 0\} \subset K[x]$. Pelo que constatamos, temos $I_K(\alpha) \neq \emptyset$. Ainda:

- $0(x) \in K[x]$ e $0(\alpha) = 0 \Rightarrow 0(x) \in I_K(\alpha)$.
- $f(x), g(x) \in I_K(\alpha) \Rightarrow f(x), g(x) \in K[x]$ e $f(\alpha) = g(\alpha) = 0 \Rightarrow f(x) + g(x) = (f+g)(x) \in K[x]$ e $(f+g)(\alpha) = f(\alpha) + g(\alpha) = 0 \Rightarrow (f+g)(x) \in I_K(\alpha)$.
- $f(x) \in I_K(\alpha) \subset K[x]$ e $g(x) \in K[x] \Rightarrow f(x)g(x) = (fg)(x) \in K[X]$ e $(fg)(\alpha) = f(\alpha)g(\alpha) = 0 \Rightarrow (fg)(x) \in I_K(\alpha)$.

Assim, $I_K(\alpha)$ é ideal de $K[x]$. Como $q(x) \in I_K(\alpha)$ e $q(x) \neq 0(x)$, temos $I_K(\alpha) \neq \langle 0(x) \rangle$. Sendo K um corpo, temos K domínio Euclidiano, donde, pelo Teorema 18, K é um domínio de ideais principais. Portanto, existe $p(x) \in K[x]$ tal que $I_K(\alpha) = \langle p(x) \rangle$.

Seja $p_1(x) \in K[x]$ tal que $I_K(\alpha) = \langle p_1(x) \rangle$. Então $\langle p_1(x) \rangle = \langle p(x) \rangle$. Pelo Teorema 2, segue que $p_1(x) = u(x)p(x)$, com $u(x) \in U(K[x])$. Entretanto, sabemos que $U(K[x]) = K \setminus \{0\}$, donde $p_1(x) = up(x)$, com $u \in K \setminus \{0\}$. Assim, existe único $p(x) \in k[x]$ mônico tal que $I_K(\alpha) = \langle p(x) \rangle$. Com isso, fazem sentido as seguintes definições:

Definição 45 (Polinômio mínimo de α sobre K)**.** *Sejam K um subcorpo de $\mathbb{C}$ e $\alpha \in \mathbb{C}$ algébrico sobre K. O único polinômio mônico $p(x) \in K[x]$ tal que:*

$$I_K(\alpha) = \langle p(x) \rangle$$

é chamado de polinômio mínimo de α sobre K e é denotado por $irr_K(\alpha)$.

Definição 46 (Grau de α sobre K)**.** *Sejam K um subcorpo de $\mathbb{C}$ e $\alpha \in \mathbb{C}$ algébrico sobre K. Então o grau de α sobre K, denotado por $deg_K(\alpha)$, é dado por:*

$$deg_K(\alpha) = deg(irr_K(\alpha))$$

Quando $K = \mathbb{Q}$ escrevemos $deg(\alpha)$ para representar $deg_{\mathbb{Q}}(\alpha)$.

Mostraremos agora propriedades dos polinômios mínimos, as quais serão úteis no estudo dos conjugados de um elemento sobre um corpo e no estudo de extensões de corpos.

Teorema 57. *Sejam K um subcorpo de $\mathbb{C}$ e α algébrico sobre K. Então $irr_K(\alpha)$ é irredutível em $K[x]$.*

Demonstração. Suponha que $irr_K(\alpha)$ é redutível em $K[x]$. Então existem $r(x), s(x) \in K[x] \setminus U(K[x]) \cup \{0[x]\}$ tais que:

$$irr_K(\alpha) = r(x)s(x)$$

Como $U(K[x]) \cup \{0[x]\} = K$, temos $r(x), s(x) \notin K$, donde $deg(r(x)), deg(s(x)) \geq 1$. Assim:

$$deg(irr_K(\alpha)) = deg(r(x)) + deg(s(x)) > \max(deg(r(x)), deg(s(x)))$$

Como α é uma raiz de $irr_K(\alpha)$, temos $r(\alpha)s(\alpha) = 0$, donde $r(\alpha) = 0$ ou $s(\alpha) = 0$. Sem perda de generalidade, podemos supor $r(\alpha) = 0$. Logo:

$$r(x) \in I_K(\alpha) = \langle irr_K(\alpha) \rangle$$

donde temos que $irr_K(\alpha) \mid r(x)$ e, consequentemente, $deg(r(x)) < deg(irr_K(\alpha)) \leq deg(r(x))$, o que é um absurdo. Portanto, $irr_K(\alpha)$ é irredutível em $K[x]$. □

Definamos então o conceito de conjugados sobre um corpo e provemos algumas de suas propriedades.

Definição 47 (Conjugados de α sobre K)**.** *Sejam $K \subset \mathbb{C}$ um subcorpo e $\alpha \in \mathbb{C}$ algébrico sobre K. Os conjugados de α sobre K são as raízes em $\mathbb{C}$ de $irr_K(\alpha)$.*

Teorema 58. *Sejam K um subcorpo de $\mathbb{C}$ e $\alpha \in \mathbb{C}$ algébrico sobre K. Então os conjugados de α sobre K são distintos.*

Demonstração. Suponha que α tem dois conjugados sobre K iguais. Então $irr_K(\alpha)$ possui uma raiz de ordem ao menos 2. Seja $\beta \in \mathbb{C}$ tal raiz. Então:

$$irr_K(\alpha) = (x - \beta)^2 r(x)$$

com $r(x) \in \mathbb{C}[x]$. Derivando a equação acima, obtemos:

$$irr_K(\alpha)' = (x - \beta)^2 r'(x) + 2(x - \beta)r(x)$$

donde $irr_K(\alpha)'(\beta) = 0$. Como $irr_K(\alpha)' \in K[x]$, temos $irr_K(\alpha)' \in I_K(\alpha) = \langle irr_K(\alpha) \rangle$. Logo:

$$irr_K(\alpha) \mid irr_K(\alpha)'$$

e, consequentemente, $deg(irr_K(\alpha)) \leq deg((irr_K(\alpha)'))$, o que é um absurdo. Portanto, os conjugados de α sobre K são distintos. □

Teorema 59. *Se α é um inteiro algébrico então seus conjugados sobre $\mathbb{Q}$ também são inteiros algébricos.*

Demonstração. Como α é um inteiro algébrico, existe $h(x) \in \mathbb{Z}[x]$ mônico tal que $h(\alpha) = 0$. Como $h(x) \in \mathbb{Q}[x]$, temos $I_{\mathbb{Q}}(\alpha) = \langle irr_{\mathbb{Q}}(\alpha) \rangle$ tal que:

$$h(x) = irr_{\mathbb{Q}}(\alpha)q(x)$$

para algum $q(x) \in \mathbb{Q}[x]$. Seja β um conjugado de α sobre $\mathbb{Q}$. Então β também é raiz de $irr_{\mathbb{Q}}(\alpha)$. Logo $h(\beta) = 0$ e assim β é também inteiro algébrico. □

Por fim, provaremos um teorema que será essencial para expressarmos os elementos de extensões de corpos de maneira mais simples.

Teorema 60. *Se α é um inteiro algébrico então:*

$$irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$$

Demonstração. Sejam $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n \in \mathbb{Q}$ os conjugados de α sobre $\mathbb{Q}$. Então:

$$\begin{aligned} irr_{\mathbb{Q}}(\alpha) &= (x - \alpha_1)(x - \alpha_2)...(x - \alpha_n) \\ &= x^n - (\alpha_1 + \alpha_2 + ... + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n)x^{n-2} + \\ &+ ... + (-1)^n\alpha_1\alpha_2...\alpha_n \end{aligned}$$

Como $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$, temos:

$$\alpha_1 + ... + \alpha_n \in \mathbb{Q}$$
$$\alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n \in \mathbb{Q}$$
$$...$$
$$\alpha_1\alpha_2...\alpha_n \in \mathbb{Q}$$

Pelo teorema anterior, $\alpha_1, ..., \alpha_n$ são inteiros algébricos. Pelo Corolário 5, $\alpha_1 + ... + \alpha_n$, $\alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n$, ..., e $\alpha_1\alpha_2...\alpha_n$ são inteiros algébricos. Como eles são também racionais, pela Proposição 16 devemos ter $\alpha_1 + ... + \alpha_n$, $\alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n$, ..., e $\alpha_1\alpha_2...\alpha_n$ inteiros. Portanto, $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. □

4.2 INTEIROS ALGÉBRICOS EM CORPOS QUADRÁTICOS

Primeiramente, analisaremos o corpo $\mathbb{Q}(\alpha)$ obtido ao adjuntar uma raiz $\alpha \in \mathbb{C}$ de um polinômio quadrático irredutível $x^2 + ax + b \in \mathbb{Q}[x]$ a $\mathbb{Q}$. Isto é, $\mathbb{Q}(\alpha)$ é o menor subcorpo de $\mathbb{C}$ contendo ambos $\mathbb{Q}$ e α. Mais formalmente:

Definição 48. *Dado $\alpha \in \mathbb{C}$ raiz de $x^2 + ax + b \in \mathbb{Q}[x]$ irredutível sobre $\mathbb{Q}$, definimos* $\mathbb{Q}(\alpha) = \bigcap_{\substack{K(corpo) \subset \mathbb{C} \\ \mathbb{Q} \subset K, \alpha \in K}} K$.

Vale a pena notar que, como $x^2 + ax + b$ é irredutível em $\mathbb{Q}[x]$, temos $\alpha \notin \mathbb{Q}$.

Mostremos que $\mathbb{Q}(\alpha)$ é um corpo. Seja $A = \{K \subset \mathbb{C} \mid K \text{ é corpo}, \mathbb{Q} \subset K, \alpha \in K\}$. Dados $a, b \in \mathbb{Q}(\alpha) = \bigcap_{K \in A} K$, e $c \in \mathbb{Q}(\alpha) \setminus \{0\}$, temos:

- $a + b \in \mathbb{Q}(\alpha)$: Como $a, b \in Q(\alpha) = \bigcap_{K \in A} K$, temos $a, b \in K \ \forall \ K \in A \Rightarrow a + b \in K \ \forall \ K \in A \Rightarrow a + b \in \bigcap_{K \in A} K = \mathbb{Q}(\alpha)$.
- $ab \in \mathbb{Q}(\alpha)$: Como $a, b \in Q(\alpha) = \bigcap_{K \in A} K$, temos $a, b \in K \ \forall \ K \in A \Rightarrow ab \in K \ \forall \ K \in A \Rightarrow ab \in \bigcap_{K \in A} K = \mathbb{Q}(\alpha)$.
- $-a \in \mathbb{Q}(\alpha)$: Como $a \in Q(\alpha) = \bigcap_{K \in A} K$, temos $a \in K \ \forall \ K \in A \Rightarrow -a \in K \ \forall \ K \in A \Rightarrow -a \in \bigcap_{K \in A} K = \mathbb{Q}(\alpha)$.
- $c^{-1} \in \mathbb{Q}(\alpha)$: Como $c \in Q(\alpha) = \bigcap_{K \in A} K$, temos $c \in K \ \forall \ K \in A \Rightarrow c^{-1} \in K \ \forall \ K \in A \Rightarrow c^{-1} \in \bigcap_{K \in A} K = \mathbb{Q}(\alpha)$.
- $\mathbb{Q} \subset \mathbb{Q}(\alpha), \alpha \in \mathbb{Q}(\alpha)$: Como $\mathbb{Q} \subset K \ \forall \ K \in A \Rightarrow \mathbb{Q} \subset \bigcap_{K \in A} K = \mathbb{Q}(\alpha)$. Analogamente, $\alpha \in K \ \forall \ K \in A \Rightarrow \alpha \in \bigcap_{K \in A} K = \mathbb{Q}(\alpha)$.

Como $\mathbb{Q}(\alpha) \subset \mathbb{C}$, o restante das propriedades de um corpo segue do fato de $\mathbb{C}$ ser um corpo.

Agora, vamos caracterizar o corpo $\mathbb{Q}(\alpha)$. Considere o conjunto $B = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$. Pela definição de B, segue que $\mathbb{Q} \subset B$ e $\alpha \in B$. Mostremos que B é um corpo. Sejam $x, y \in B$:

- $x + y \in B$: Temos $x = a + b\alpha$ e $y = c + d\alpha$ com $a, b, c, d \in \mathbb{Q}$. Assim:

  $$x + y = a + b\alpha + c + d\alpha = (a + c) + (b + d)\alpha$$

  e $a + c, b + d \in \mathbb{Q}$, donde $x + y \in B$.

- $xy \in B$: Temos $x = a + b\alpha$ e $y = c + d\alpha$ com $a, b, c, d \in \mathbb{Q}$. Assim:

  $$xy = (a + b\alpha)(c + d\alpha) = ac + (bc + ad)\alpha + bd\alpha^2$$

  Como existem $u, v \in \mathbb{Q}$ tais que $\alpha^2 + u\alpha + v = 0$, temos $\alpha^2 = -u\alpha - v$. Logo:

  $$xy = ac+(bc+ad)\alpha+bd\alpha^2 = ac+(bc+ad)\alpha-bdu\alpha-bdv = (ac-bdv)+(bc+ad-bdu)\alpha$$

  e $ac - bdv, bc + ad - bdu \in \mathbb{Q}$, donde $xy \in B$.

- $x \neq 0 \Rightarrow x^{-1} \in B$: Como $x \in B \setminus \{0\}$, temos $x = a + b\alpha$ com a e b não simultaneamente nulos. Sabemos ainda que existem $u, v \in \mathbb{Q}$ tais que $\alpha^2 + u\alpha + v = 0$. Afirmo que $a^2 - uab + vb^2 \neq 0$. De fato, suponha $a^2 - uab + vb^2 = 0$. Caso $a = 0$, temos então $vb^2 = 0$ e $v \neq 0$ (pois $x^2 + ux + v$ é irredutível em $\mathbb{Q}[x]$), donde $b = 0$, o

que contradiz $(a, b) \neq (0, 0)$. Analogamente, se $b = 0$, temos $a^2 = 0$, donde $a = 0$, o que é um absurdo. Por fim, caso $a, b \neq 0$, temos:

$$a^2 - uab + vb^2 = 0$$
$$\left(\frac{a}{b}\right)^2 - u\frac{a}{b} + v = 0$$
$$\left(-\frac{a}{b}\right)^2 + u\left(-\frac{a}{b}\right) + v = 0$$

donde $-\frac{a}{b} \in \mathbb{Q}$ é raiz de $x^2 + ux + v \in \mathbb{Q}[x]$, o que é um absurdo pois $x^2 + ux + v$ é irredutível em $\mathbb{Q}[x]$. Logo, $a^2 - uab + vb^2 \neq 0$. Note ainda que:

$$(a + b\alpha)(a - b\alpha - ub) = a^2 - b^2\alpha^2 - uab - ub^2\alpha =$$
$$= a^2 - b^2(-u\alpha - v) - uab - ub^2\alpha = a^2 - uab + vb^2$$

Portanto:

$$x^{-1} = \frac{1}{x} = \frac{1}{a + b\alpha} = \frac{a - b\alpha - ub}{(a + b\alpha)(a - b\alpha - ub)} = \left(\frac{a - ub}{a^2 - uab + vb^2}\right) + \alpha\left(\frac{-b}{a^2 - uab + vb^2}\right)$$

com $\left(\frac{a - ub}{a^2 - uab + vb^2}\right), \left(\frac{-b}{a^2 - uab + vb^2}\right) \in \mathbb{Q}$, donde $x^{-1} \in B$.

Como $\mathbb{Q} \subset B \subset \mathbb{C}(corpo)$ e $\alpha \in B$, segue que B é subcorpo de $\mathbb{C}$ que contém $\mathbb{Q}$ e α. Portanto, $\mathbb{Q}(\alpha) \subset B$.

Por outro lado, se $\mathbb{Q} \subset K(subcorpo) \subset \mathbb{C}$ e $\alpha \in K$, então $a + b\alpha \in K$ para todos $a, b \in \mathbb{Q}$, donde $B \subset \bigcap_{\substack{K(corpo)\subset\mathbb{C} \\ \mathbb{Q}\subset K, \alpha\in K}} K = \mathbb{Q}(\alpha)$.

Dessa forma, segue que $\mathbb{Q}(\alpha) = B = \{a + b\alpha \mid a, b \in \mathbb{Q}\}$.

Conseguimos, pela construção anterior, encontrar uma forma para os elementos de $\mathbb{Q}(\alpha)$. Esta forma, no entanto, não é única, como veremos no seguinte lema, complementado pelo autor deste texto:

Lema 7. *Dados $\alpha \in \mathbb{C}$ raiz de $x^2 + ax + b \in \mathbb{Q}[x]$ irredutível e $u, v \in \mathbb{Q}, v \neq 0$, temos:*

$$\mathbb{Q}(\alpha) = \mathbb{Q}(u + v\alpha)$$

Demonstração. Devido as considerações anteriores, para provar este lema basta mostrarmos que $\alpha \in \mathbb{Q}(u + v\alpha)$ e $u + v\alpha \in \mathbb{Q}(\alpha)$. Como $\mathbb{Q}(\alpha) = \{x + y\alpha \mid x, y \in \mathbb{Q}\}$ e $u, v \in \mathbb{Q}$, segue que $u + v\alpha \in \mathbb{Q}(\alpha)$. Por outro lado, como $v \in \mathbb{Q} \setminus \{0\}$, temos $v^{-1} \in \mathbb{Q}$, donde $\alpha = v^{-1}(-u + (u + v\alpha)) \in \mathbb{Q}(u + v\alpha)$.

Portanto, $\mathbb{Q}(\alpha) = \mathbb{Q}(u + v\alpha)$. □

Além de mostrar que a forma não é única, o lema anterior nos permite reescrever o conjunto $\mathbb{Q}(\alpha)$ de outras maneiras, o que é útil para simplificar a expressão dentro do parênteses e impor condições sobre α, como veremos no próximo resultado.

Teorema 61. *Seja K um corpo quadrático. Então existe único $m \in \mathbb{Z}$ livre de quadrados tal que $K = \mathbb{Q}(\sqrt{m})$.*

Demonstração. Como K é corpo quadrático, existe um polinômio $x^2 + ax + b \in \mathbb{Q}[x]$ irredutível em $\mathbb{Q}[x]$ e $\alpha \in \mathbb{C}$ tal que $\alpha^2 + a\alpha + b = 0$ e $K = \mathbb{Q}(\alpha)$. Como as raízes de $x^2 + ax + b$ em $\mathbb{C}$ são:

$$\alpha_1 = \frac{-a + \sqrt{a^2 - 4b}}{2} \text{ e } \alpha_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}$$

temos $\alpha = \alpha_1$ ou α_2. Note que $\alpha_1 + \alpha_2 = -a \in \mathbb{Q}$, donde $\alpha_1 = -a - \alpha_2 \in \mathbb{Q}(\alpha_2)$ e $\alpha_2 = -a - \alpha_1 \in \mathbb{Q}(\alpha_1)$. Consequentemente, $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$.

Portanto, $K = \mathbb{Q}\left(\frac{-a + \sqrt{a^2 - 4b}}{2}\right) = \mathbb{Q}(\sqrt{a^2 - 4b})$. De fato, $\frac{-a + \sqrt{a^2 - 4b}}{2} = \frac{-a}{2} + \frac{1}{2}\sqrt{a^2 - 4b}$, com $\frac{-a}{2} \in \mathbb{Q}$, donde $\frac{-a + \sqrt{a^2 - 4b}}{2} \in \mathbb{Q}(\sqrt{a^2 - 4b})$. Por outro lado, como $a \in \mathbb{Q}$, temos $\sqrt{a^2 - 4b} = 2\left(\frac{a}{2} + \frac{-a + \sqrt{a^2 - 4b}}{2}\right) \in \mathbb{Q}\left(\frac{-a + \sqrt{a^2 - 4b}}{2}\right)$, donde segue a afirmação. Note que $c = a^2 - 4b \in \mathbb{Q}$ não é o quadrado de um número racional, uma vez que, caso isso ocorresse, teríamos $\alpha_1 \in \mathbb{Q}$ e $x^2 + ax + b$ seria redutível em $\mathbb{Q}[x]$. Podemos escrever c como sendo $c = \frac{p}{q}$, com $(p, q) = 1$, $q > 0$ e $p \neq 0$, de forma que $pq \neq 0$. Pela Proposição 14, temos que existem únicos $d, l \in \mathbb{N}^*$ e $u \in \{-1, 1\}$ tais que $pq = ud^2l$. Utilizando o Lema 7, segue que:

$$\begin{aligned} K = \mathbb{Q}\left(\sqrt{c}\right) = \mathbb{Q}\left(\sqrt{\frac{p}{q}}\right) = \mathbb{Q}\left(q\sqrt{\frac{p}{q}}\right) = \mathbb{Q}\left(\sqrt{pq}\right) = \mathbb{Q}\left(\sqrt{ud^2l}\right) = \mathbb{Q}\left(d\sqrt{ul}\right) = \\ = \mathbb{Q}\left(\sqrt{ul}\right) = \mathbb{Q}\left(\sqrt{m}\right) \end{aligned}$$

com $m = ul \in \mathbb{Z} \setminus \{0, 1\}$ livre de quadrados ($m \neq 1$ pois $m = 1$ implica em $pq = d^2 \Rightarrow c = \frac{p}{q} = \frac{d^2}{q^2} = \left(\frac{d}{q}\right)^2$, donde c seria o quadrado de um racional).

Seja $n \in \mathbb{Z}$ livre de quadrados tal que $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ (note que $n \neq 1$, pois $n = 1$ implicaria em $x^2 + ax + b$ redutível em $\mathbb{Q}[x]$). Então $\sqrt{m} = x + y\sqrt{n}$ com $x, y \in \mathbb{Q}$. Elevando a igualdade ao quadrado, obtemos:

$$m = x^2 + ny^2 + 2xy\sqrt{n}$$

Caso $xy \neq 0$, temos:

$$\sqrt{n} = \frac{m - x^2 - ny^2}{2xy} \in \mathbb{Q}$$

o que contradiz $\sqrt{n} \notin \mathbb{Q}$, uma vez que $n \in \mathbb{Z}$ é livre de quadrados. Logo $xy = 0$. Caso $y = 0$, teríamos $\sqrt{m} = x \in \mathbb{Q}$, o que é um absurdo pois $m \neq 1$ é livre de quadrados. Assim, $x = 0$ e:

$$m = y^2 n$$

Como $y = \dfrac{t}{w}$, com $t, w \in \mathbb{Z}, t, w \neq 0$ (pois $y \neq 0$) e $(t, w) = 1$, temos:

$$w^2 m = t^2 n$$

Do fato $(t, w) = 1$, temos $t^2 | m$. Mas m é livre de quadrados, donde devemos ter $t^2 = 1$. Analogamente, temos $w^2 | n$ e n livre de quadrados implicando em $w^2 = 1$. Portanto, $m = n$ e, consequentemente, m está unicamente determinado para cada K. □

O próximo resultado, que será usado nos próximos capítulos, nos mostra que os inteiros algébricos de certos corpos quadráticos são exatamente os domínios $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ e $\mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right)$. Tal fato nos permitirá obter resultados sobre estes domínios, uma vez que o conjunto de inteiros algébricos em um corpo K satisfaz propriedades importantes, como veremos mais adiante.

Teorema 62. *Sejam K um corpo quadrático e $m \in \mathbb{Z}$ livre de quadrados tal que $K = \mathbb{Q}(\sqrt{m})$. O conjunto O_K de inteiros algébricos em K é dado por:*

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{se } m \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right), & \text{se } m \equiv 1 \pmod 4 \end{cases}$$

Demonstração. Sabemos que $\mathbb{Z} + \mathbb{Z}\sqrt{m}$ e $\mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right)$ (caso $m \equiv 1 \pmod 4$) são inteiros algébricos. Ainda, se $m \not\equiv 1 \pmod 4$, dado $z = a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$, temos z da forma $a + b\sqrt{m}$, com $a, b \in \mathbb{Q}$, donde $\mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right) \subset O_K$. Analogamente, se $m \equiv 1 \pmod 4$, temos $z \in \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right) \Rightarrow z = a + b\left(\dfrac{1+\sqrt{m}}{2}\right)$ com $a, b \in \mathbb{Z}$. Como $\left(\dfrac{1+\sqrt{m}}{2}\right) = \dfrac{1}{2} + \dfrac{\sqrt{m}}{2} \in \mathbb{Q}(\sqrt{m})$, temos $z \in \mathbb{Q}(\sqrt{m})$. Assim, $\mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right) \subset O_K$.

Vamos agora mostrar a inclusão oposta. Seja $\alpha \in O_K \subset K$, de forma que $\alpha = a + b\sqrt{m}$ com $a, b \in \mathbb{Q}$. Então α é raiz de:

$$x^2 - 2ax + (a^2 - mb^2) \in \mathbb{Q}[x]$$

O discriminante deste polinômio é:

$$(2a)^2 - 4(a^2 - mb^2) = 4mb^2$$

de forma que $x^2 - 2ax + (a^2 - mb^2)$ é redutível em $\mathbb{Q}[x]$ se, e somente se, $b = 0$, uma vez que $\sqrt{4mb^2} = 2|b|\sqrt{m}$, $2|b| \in \mathbb{Q}$ e $\sqrt{m} \notin \mathbb{Q}$, de forma que $2|b|\sqrt{m} \in \mathbb{Q}$ se, e somente se, $2|b| = 0$, isto é, $b = 0$. Portanto:

$$irr_{\mathbb{Q}}(\alpha) = \begin{cases} x - a, & \text{se } b = 0 \\ x^2 - 2ax + (a^2 - mb^2), & \text{se } b \neq 0 \end{cases}$$

Como α é um inteiro algébrico, temos pelo Teorema 60 que $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$. Assim:

$$\begin{cases} a \in \mathbb{Z}, & \text{se } b = 0 \\ 2a, a^2 - mb^2 \in \mathbb{Z}, & \text{se } b \neq 0 \end{cases}$$

Se $b = 0$, temos $\alpha = a \in \mathbb{Z} \subset \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Suponha que $b \neq 0$. Se $2a \in 2\mathbb{Z}$ então $a \in \mathbb{Z}$ e, consequentemente, $mb^2 \in \mathbb{Z}$. Como m é livre de quadrados e $b \in \mathbb{Q}$, temos $b \in \mathbb{Z}$. De fato, como $b = \frac{p}{q}$ com $p, q \in \mathbb{Z}, p \neq 0, q > 0$ e $(p, q) = 1$, temos $\frac{mp^2}{q^2} \in \mathbb{Z}$, donde $q^2 | mp^2$ e $(p^2, q^2) = 1 \Rightarrow q^2 | m$ e m é livre de quadrados $\Rightarrow q^2 = 1 \Rightarrow q = 1 \Rightarrow b = p \in \mathbb{Z}$. Assim, temos $\alpha = a + b\sqrt{m} \in \mathbb{Z} + \mathbb{Z}\sqrt{m}$. Se $2a \in 2\mathbb{Z} + 1$, temos $a = \frac{2k+1}{2}$, com $k \in \mathbb{Z}$. Como $a^2 - mb^2 \in \mathbb{Z}$, temos $4\left(\left(\frac{2k+1}{2}\right)^2 - mb^2\right) = (2k+1)^2 - 4mb^2 \in \mathbb{Z}$, donde $4mb^2 \in \mathbb{Z}$. Do fato de que m é livre de quadrados e $b \in \mathbb{Q}$, segue por um argumento semelhante ao anterior que $2b \in \mathbb{Z}$. Caso $b \in \mathbb{Z}$, temos:

$$a^2 = (a^2 - mb^2) + mb^2 \in \mathbb{Z}$$

o que contradiz $a = \frac{2k+1}{2}$. Portanto $b \notin \mathbb{Z}$, de forma que $2b \in 2\mathbb{Z} + 1$ e $b = \frac{2v+1}{2}$, com $v \in \mathbb{Z}$. Então:

$$\begin{aligned} a^2 - mb^2 &= \frac{1}{4}((2k+1)^2 - m(2v+1)^2) \\ a^2 - mb^2 &= \frac{1}{4}(4k^2 + 4k + 1 - 4m(v^2 + v) - m) \\ a^2 - mb^2 &= k^2 + k - m(v^2 + v) + \frac{1-m}{4} \\ \frac{m-1}{4} &= k^2 + k - m(v^2 + v) - (a^2 - mb^2) \in \mathbb{Z} \end{aligned}$$

donde $m \equiv 1 \pmod 4$ e:

$$\begin{aligned} \alpha = a + b\sqrt{m} &= \frac{2k+1}{2} + \frac{2v+1}{2}\sqrt{m} \\ &= (k - v) + (2v + 1)\left(\frac{1+\sqrt{m}}{2}\right) \in \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right) \end{aligned}$$

Portanto, $O_K \subset \mathbb{Z} + \mathbb{Z}\sqrt{m}$ caso $m \not\equiv 1 \pmod 4$ e $O_K \subset \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$ caso $m \equiv 1 \pmod 4$. Pelas considerações anteriores, segue que:

$$O_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & \text{se } m \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right), & \text{se } m \equiv 1 \pmod 4 \end{cases}$$

□

4.3 EXTENSÕES SIMPLES

Generalizaremos os resultados obtidos sobre corpos quadráticos para outros tipos de extensões. Em particular, começaremos estudando as propriedades de extensões simples, antes de analisar as extensões múltiplas.

Definição 49 (Extensão simples)**.** *Sejam $K \subset \mathbb{C}$ um subcorpo de $\mathbb{C}$ e $\alpha \in \mathbb{C}$. Definimos:*

$$K(\alpha) = \bigcap_{\substack{\alpha \in F \\ K \subseteq F(subcorpo) \subseteq \mathbb{C}}} F \tag{4.1}$$

como sendo uma extensão simples de K.

Note que $K(\alpha) \neq \emptyset$, uma vez que $\alpha \in \mathbb{C}$, $K \subset \mathbb{C}$ e $\mathbb{C}$ é subcorpo de $\mathbb{C}$, donde o conjunto de elementos sobre os quais estamos tomando a intersecção é não vazio. Como todos esses elementos contém α, segue que a intersecção é não vazia.

Mostremos que $K(\alpha)$ é um corpo. Seja $A = \{F \subset \mathbb{C} \mid F \text{ é subcorpo de } \mathbb{C}, K \subset F, \alpha \in F\}$. Dados $a, b \in K(\alpha), c \in K(\alpha) \setminus \{0\}$, temos:

- $a + b \in K(\alpha)$: Como $a, b \in K(\alpha) = \bigcap_{\substack{F(subcorpo) \subset \mathbb{C} \\ K \subset F, \alpha \in F}} F$, temos $a, b \in F \ \forall \ F \in A \Rightarrow a + b \in F \ \forall \ F \in A \Rightarrow a + b \in \bigcap_{F \in A} F = K(\alpha)$.
- $ab \in K(\alpha)$: Como $a, b \in K(\alpha) = \bigcap_{\substack{F(subcorpo) \subset \mathbb{C} \\ K \subset F, \alpha \in F}} F$, temos $a, b \in F \ \forall \ F \in A \Rightarrow ab \in F \ \forall \ F \in A \Rightarrow ab \in \bigcap_{F \in A} F = K(\alpha)$.
- $-a \in K(\alpha)$: Como $a \in K(\alpha) = \bigcap_{\substack{F(subcorpo) \subset \mathbb{C} \\ K \subset F, \alpha \in F}} F$, temos $a \in F \ \forall \ F \in A \Rightarrow -a \in F \ \forall \ F \in A \Rightarrow -a \in \bigcap_{F \in A} F = K(\alpha)$.
- $c^{-1} \in K(\alpha)$: Como $c \in K(\alpha) = \bigcap_{\substack{F(subcorpo) \subset \mathbb{C} \\ K \subset F, \alpha \in F}} F$, temos $c \in F \ \forall \ F \in A \Rightarrow c^{-1} \in F \ \forall \ F \in A \Rightarrow c^{-1} \in \bigcap_{F \in A} F = K(\alpha)$.
- $K \subset K(\alpha), \alpha \in K(\alpha)$: Como $K \subset F \ \forall \ F \in A \Rightarrow K \subset \bigcap_{F \in A} F = K(\alpha)$. Analogamente, $\alpha \in F \ \forall \ F \in A \Rightarrow \alpha \in \bigcap_{F \in A} F = K(\alpha)$.

Como $K(\alpha) \subset \mathbb{C}$, o restante das propriedades de um corpo segue do fato de $\mathbb{C}$ ser um corpo.

Note que $K(\alpha) = K \Leftrightarrow \alpha \in K$.

Dados $K(subcorpo) \subset \mathbb{C}$ e $\alpha \in \mathbb{C}$, seja L o conjunto:

$$\left\{\frac{b_0+b_1\alpha+...+b_m\alpha^m}{c_0+c_1\alpha+...+c_n\alpha^n} \mid m,n\in\mathbb{N}, b_0,...,b_m,c_0,...,c_n\in K, c_0+c_1\alpha+...+c_n\alpha^n\neq 0\right\}$$
$$=\left\{\frac{f(\alpha)}{g(\alpha)} \mid f(x),g(x)\in K[x], g(\alpha)\neq 0\right\}$$

Mostremos que L é um corpo. De fato, as propriedades da soma e do produto (e a não existência de divisores de 0) são satisfeitas pois $L\subset\mathbb{C}(corpo)$. Ainda, dado $k\in K$, seja $k(x)\in K[x]$ dado por $k(x)=k\ \forall\ x\in K$, de forma que $\frac{k(\alpha)}{1(\alpha)}=\frac{k}{1}=k\in L$, donde $K\subset L$. Analogamente, como $f(x)=x\in K[x]$, temos $\frac{f(\alpha)}{1(\alpha)}=\frac{\alpha}{1}=\alpha\in L$. Por fim, dados $a,b\in L$ e $c\in L\setminus\{0\}$, temos:

- $a+b\in L$: Existem $f(x),g(x),p(x),q(x)\in K[x]$ tais que $g(\alpha),q(\alpha)\neq 0$ e $a=\frac{f(\alpha)}{g(\alpha)}$ e $b=\frac{p(\alpha)}{q(\alpha)}$. Logo:

  $$a+b=\frac{f(\alpha)}{g(\alpha)}+\frac{p(\alpha)}{q(\alpha)}=\frac{f(\alpha)q(\alpha)+g(\alpha)p(\alpha)}{g(\alpha)q(\alpha)}=\frac{(fq+gp)(\alpha)}{(gq)(\alpha)}\in L$$

  uma vez que K corpo implica em $K[x]$ domínio de integridade, donde $(fq+gp)(x),(gq)(x)\in K[x]$ e $g(\alpha)q(\alpha)\neq 0$, dado que $g(\alpha),q(\alpha)\in\mathbb{C}\setminus\{0\}$ e $\mathbb{C}$ não possui divisores de 0.

- $ab\in L$: Existem $f(x),g(x),p(x),q(x)\in K[x]$ tais que $g(\alpha),q(\alpha)\neq 0$ e $a=\frac{f(\alpha)}{g(\alpha)}$ e $b=\frac{p(\alpha)}{q(\alpha)}$. Logo:

  $$ab=\frac{f(\alpha)}{g(\alpha)}\frac{p(\alpha)}{q(\alpha)}=\frac{(fp)(\alpha)}{gq(\alpha)}\in L$$

  uma vez que $K[x]$ é domínio de integridade, donde $(fp)(x),(gq)(x)\in K[x]$, e $\mathbb{C}$ não possui divisores de 0, donde $(gq)(\alpha)\neq 0$. Note que, como $-1\in K\subset L$, segue dessa propriedade que se $d\in L$, então $-d\in L$.

- $c^{-1}\in L$: Existem $f(x),g(x)\in K[x]$ tais que $g(\alpha)\neq 0$ e $c=\frac{f(\alpha)}{g(\alpha)}$. Ainda, como $c\neq 0$, devemos ter $f(\alpha)\neq 0$. Consequentemente, $d=\frac{g(\alpha)}{f(\alpha)}\in L$ e:

  $$cd=\frac{f(\alpha)}{g(\alpha)}\frac{g(\alpha)}{f(\alpha)}=1$$

  donde $c^{-1}=d\in L$.

Com isso, vemos que L é um corpo que contém K e α. Consequentemente, temos $K(\alpha)\subset L$. Por outro lado, seja F um subcorpo de $\mathbb{C}$ que contenha K e α. Então,

dado $f(x) \in K[x]$, temos $f(\alpha) \in F$. Seja $a \in L$. Existem $f(x), g(x) \in K[x]$ tais que $g(\alpha) \neq 0$ e $a = \dfrac{f(\alpha)}{g(\alpha)}$. Como $f(\alpha), g(\alpha) \in F$, $g(\alpha) \neq 0$ e F é um corpo, devemos ter $g(\alpha)^{-1} = \dfrac{1}{g(\alpha)} \in F$, donde $a = \dfrac{f(\alpha)}{g(\alpha)} = f(\alpha)\dfrac{1}{g(\alpha)} \in F$. Portanto, $L \subset F$ para todo $F \in \{F \subset \mathbb{C} \mid F \text{ é subcorpo de } \mathbb{C}, K \subset F, \alpha \in F\}$. Assim: $L \subset \bigcap_{\substack{F(subcorpo)\subset\mathbb{C} \\ K\subset F, \alpha\in F}} F = K(\alpha)$.

Dessa forma, temos $K(\alpha) = L$.

Analisemos agora o caso em que $\alpha \in \mathbb{C}$ é algébrico sobre K. Seja $n = deg_K(\alpha)$. Sabemos que, dado $a \in K$, existem $f(x), g(x) \in K[x]$ tais que $g(\alpha) \neq 0$ e $a = \dfrac{f(\alpha)}{g(\alpha)}$. Como $g(\alpha) \neq 0$, temos $irr_K(\alpha) \nmid g(x)$. Uma vez que $irr_K(\alpha)$ é irredutível em $K[x]$, que é um domínio Euclidiano (pois K é corpo) e, consequentemente, é domínio de ideais principais pelo Teorema 18, temos:

$$\langle irr_K(\alpha), g(x)\rangle = \langle 1\rangle = K[x]$$

Portanto, podemos encontrar $m(x), n(x) \in K[x]$ tais que:

$$m(x)irr_K(\alpha) + n(x)g(x) = 1$$

Disso, segue-se que:

$$n(\alpha)g(\alpha) = 1 \Rightarrow \frac{1}{g(\alpha)} = n(\alpha) \Rightarrow a = \frac{f(\alpha)}{g(\alpha)} = f(\alpha)n(\alpha)$$

Assim, todo elemento $a \in K(\alpha)$ pode ser escrito como $h(\alpha)$, com $h(x) \in K[x]$. Como $K[x]$ é domínio Euclidiano, podemos dividir $h(x)$ por $irr_K(\alpha)$, de forma que existem $u(x), v(x) \in K[x]$ tais que:

$$h(x) = u(x)irr_K(\alpha) + v(x), deg(v(x)) < deg(irr_K(\alpha)) = n$$

Como α é raiz de $irr_K(\alpha)$, temos:

$$a = h(\alpha) = v(\alpha) = a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}, a_0, a_1, ..., a_{n-1} \in K$$

Com isso, provamos o seguinte teorema:

Teorema 63. *Sejam $K(subcorpo) \subset \mathbb{C}$, $\alpha \in \mathbb{C}$ algébrico sobre K e $n = deg_K(\alpha)$. Então:*

$$K(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \mid a_0, ..., a_{n-1} \in K\}$$

Note que o teorema anterior generaliza a construção feita para corpos quadráticos. De fato, o caso para corpos quadráticos é o caso particular do teorema anterior em que $K = \mathbb{Q}$ e $irr_{\mathbb{Q}}(\alpha)$ é um polinômio quadrático. Ainda, o resultado anterior justifica a seguinte definição:

Definição 50 (Grau de uma extensão $K(\alpha)$ sobre K)**.** *Sejam $K(subcorpo) \subset \mathbb{C}$, $\alpha \in \mathbb{C}$ algébrico sobre K e $deg_K(\alpha) = n$. O grau da extensão $K(\alpha)$ sobre K, denotada por $[K(\alpha) : K]$, é dada por:*

$$[K(\alpha) : K] = n$$

4.4 EXTENSÕES MÚLTIPLAS

Podemos agora estudar o que ocorre ao adjuntarmos múltiplos elementos a um corpo K. Para isso, definiremos extensões múltiplas de maneira recursiva. Sejam $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{C}$ algébricos sobre K. Definimos:

$$K(\alpha_1, \alpha_2) = K(\alpha_1)(\alpha_2)$$
$$K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2)(\alpha_3)$$
$$...$$
$$K(\alpha_1, \alpha_2, ..., \alpha_k) = K(\alpha_1, \alpha_2, ..., \alpha_{k-1})(\alpha_k)$$

Mostraremos que o estudo de extensões múltiplas pode ser reduzido ao estudo de extensões simples. Tal teorema será o principal desta seção e tem como consequência o fato de que os resultados provados para extensões simples valem também para extensões múltiplas. Para mostrar isso, antes provaremos dois lemas, propostos pelo autor deste texto:

Lema 8. *Sejam K um corpo e $p(x), q(x) \in K[x]$. Então $p(q(x)) = p \circ q(x) \in K[x]$.*

Demonstração. Sabemos que existem $a_0, a_1, ..., a_n \in K$ tais que $p(x) = \sum_{i=0}^{n} a_i x^i$. Como K é corpo, temos $K[x]$ domínio de integridade. Consequentemente:

$$q(x) \in K[x] \Rightarrow q(x) * q(x) = q(x)^2 \in K[x]$$
$$q(x)^2, q(x) \in K[x] \Rightarrow q(x)^2 * q(x) = q(x)^3 \in K[x]$$
$$...$$
$$q(x)^{n-1}, q(x) \in K[x] \Rightarrow q(x)^{n-1} * q(x) = q(x)^n \in K[x]$$

Dado $i \in \{0, ..., n\}$, como $a_i, q(x)^i \in K[x]$ (sendo $q(x)^0 = 1$), temos $a_i q(x)^i \in K[x]$.

Portanto, $a_0, a_1 q(x), a_2 q(x)^2, ..., a_n q(x)^n \in K[x] \Rightarrow a_0 + a_1 q(x) + a_2 q(x)^2 + ... + a_n q(x)^n = \sum_{i=0}^{n} a_i q(x)^i = p(q(x)) \in K[x]$. □

Lema 9. *Seja K um subcorpo de $\mathbb{C}$. Então $\mathbb{Q} \subset K$.*

Demonstração. Como K é subcorpo de $\mathbb{C}$, temos que $0, 1 \in K$. Suponha que $n \in \mathbb{N} \cap K$. Dado que K é corpo, temos K fechado para a adição, donde $n, 1 \in K \Rightarrow n + 1 \in K$. Concluímos que $n + 1 \in \mathbb{N} \cap K$. Pelo princípio de indução, segue que $n \in \mathbb{N} \cap K \ \forall \ n \in \mathbb{N}$, isto é, $\mathbb{N} \subset K$. Da propriedade do inverso aditivo, sabemos que $a \in K \Rightarrow -a \in K$. Como $\mathbb{N} \subset K$, temos $-\mathbb{N} \subset K$ e, consequentemente, $\mathbb{Z} \subset K$. Por fim, usaremos a propriedade de que todo elemento não nulo de K possui inverso multiplicativo, isto é, dado $a \in K \setminus \{0\}$, existe $a^{-1} = \frac{1}{a} \in K$. Portanto, dado $z \in \mathbb{Z} \setminus 0$, temos $\frac{1}{z} \in K$.

Seja $a \in \mathbb{Q}$ dado. Existem $p, q \in \mathbb{Z}$, com $q \neq 0$, tais que $a = \frac{p}{q}$. Pelo que provamos, $p, \frac{1}{q} \in K$. Como K é fechado para o produto, segue que $a = \frac{p}{q} = p\frac{1}{q} \in K$. Logo, $\mathbb{Q} \subset K$. □

Com isso, podemos começar a provar que as extensões múltiplas podem ser reduzidas a uma extensão simples. Faremos a demonstração para o caso da extensão com dois elementos adjuntados, a partir da qual o resultado mais geral seguirá como um corolário.

Teorema 64. *Sejam K(subcorpo) $\subset \mathbb{C}$, $\alpha, \beta \in \mathbb{C}$ algébricos sobre K. Então existe $\gamma \in \mathbb{C}$ algébrico sobre K tal que:*

$$K(\alpha, \beta) = K(\gamma)$$

Demonstração. Sejam $p(x) = irr_K(\alpha)$ e $q(x) = irr_K(\beta)$. Então:

$$p(x) = (x - \alpha_1)...(x - \alpha_m) \in K[x]$$
$$q(x) = (x - \beta_1)...(x - \beta_n) \in K[x]$$

com $\alpha_1 = \alpha, ..., \alpha_m$ conjugados de α sobre K e $\beta_1 = \beta, ..., \beta_n$ conjugados de β sobre K. Pelo Teorema 58 sabemos que os α_i são distintos, tais como os β_j. Consequentemente, o conjunto S dado por:

$$S = \left\{ \frac{\alpha_r - \alpha_s}{\beta_t - \beta_u} \mid r, s = 1, ..., m; t, u = 1, ..., n; t \neq u \right\}$$

é um subconjunto finito de $\mathbb{C}$. Seja $c \in \mathbb{Q} \setminus S$ (tal escolha é possível dado que S é finito). Vale notar que $c \neq 0$ pois $\frac{\alpha_1 - \alpha_1}{\beta_1 - \beta_n} = 0 \in S$. Então os elementos:

$$\alpha_i + c\beta_j; i = 1, ..., m; j = 1, ..., n$$

são todos distintos. De fato, caso $\alpha_i + c\beta_j = \alpha_k + c\beta_l$ com $(i, j) \neq (k, l)$, teríamos os seguintes casos:

- Caso $i = k$: Neste caso, $c\beta_j = c\beta_l$, donde segue que $c = 0$ ou $\beta_j = \beta_l$, o que são ambos absurdos, uma vez que os conjugados de β são todos distintos.
- Caso $j = l$: Neste caso, $\alpha_i = \alpha_j$, o que é um absurdo pois os conjugados de α são distintos.
- Caso $i \neq k$ e $j \neq l$: Neste caso, temos:

$$\alpha_i + c\beta_j = \alpha_k + c\beta_l$$
$$\alpha_i - \alpha_k = c(\beta_l - \beta_j)$$
$$c = \frac{\alpha_i - \alpha_k}{\beta_l - \beta_j} \in S$$

  o que é um absurdo.

Sejam $\gamma = \alpha + c\beta$, $K_1 = K(\gamma)$ e $p_1(x) = p(\gamma - cx)$. Como $K \subset K_1(corpo)$ e $p(x) \in K[x]$, temos $p(x) \in K_1[x]$. Ainda, como K_1 é subcorpo de $\mathbb{C}$, temos que $\mathbb{Q} \subset K_1$ pelo Lema 9. Consequentemente, $-c, \gamma \in K_1 \Rightarrow \gamma - cx \in K_1[x]$. Pelo Lema 8, segue que $p(\gamma - cx) = p_1(x) \in K_1[x]$. Note que $p_1(\beta) = p(\gamma - c\beta) = p(\alpha) = 0$, de forma que $p_1(x)$ e $q(x)$ possuem uma raiz em comum. Mostraremos que esta é a única raiz em comum destes polinômios. Suponha que outra raiz comum $\lambda \in \mathbb{C}$ exista. Como λ é raiz de $q(x) = (x - \beta_1)...(x - \beta_n)$, temos $\lambda = \beta_j$ para algum $j \in \{2, 3, ..., n\}$. Então:

$$p_1(\beta_j) = p(\gamma - c\beta_j) = 0$$

donde $\gamma - c\beta_j \in \{\alpha_1, ..., \alpha_m\}$. Logo, existe $k \in \{1, ..., m\}$ tal que:

$$\gamma - c\beta_j = \alpha_k$$
$$\alpha_1 + c\beta_1 - c\beta_j = \alpha_k$$
$$\alpha_1 - \alpha_k = c(\beta_j - \beta_1)$$
$$c = \frac{\alpha_1 - \alpha_k}{\beta_j - \beta_1} \in S$$

o que é um absurdo. Logo, $p_1(x)$ e $q(x)$ tem apenas β como raiz comum. Seja $h(x) = irr_{K_1}(\beta)$. Então $h(x) \mid p_1(x)$ e $h(x) \mid q(x)$. Como $p_1(x)$ e $q(x)$ tem apenas uma raiz em comum, segue que $deg(h(x)) = 1$, donde $h(x) = x + \delta$ para algum $\delta \in K_1$. E, uma vez que $h(\beta) = \beta + \delta = 0$, temos $\delta = -\beta \in K_1 \Rightarrow \beta \in K_1$. Logo, $\alpha = \gamma - c\beta \in K_1$. Com isso, mostramos que:

$$K(\alpha, \beta) \subset K_1 = K(\gamma)$$

já que $K(\gamma)$ é um subcorpo de $\mathbb{C}$ que contém K, α e β. Por outro lado, $K \subset K(\alpha, \beta)$ e $\gamma = \alpha + c\beta \in K(\alpha, \beta)$, donde conclui-se que:

$$K(\gamma) \subset K(\alpha, \beta)$$

Das duas inclusões acima, temos:

$$K(\alpha, \beta) = K(\gamma)$$

□

Note que a demonstração anterior, além de provar a validade do enunciado, nos dá uma forma de encontrar o γ que satisfaz a igualdade apresentada no teorema. Usando do que acabamos de provar, podemos então mostrar a versão mais geral do resultado:

Corolário 6. *Sejam $K(subcorpo) \subset \mathbb{C}$, $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{C}$ algébricos sobre K. Então existe $\alpha \in \mathbb{C}$ algébrico sobre K tal que:*

$$K(\alpha_1, \alpha_2, ..., \alpha_n) = K(\alpha)$$

Demonstração. Para $n = 1$ o resultado é trivial. Para $n = 2$, o resultado segue pelo teorema anterior. Suponha que o resultado valha para $n \geq 2$. Mostraremos que ele vale para $n + 1$. Sabemos que existe α tal que $K(\alpha_1, \alpha_2, ..., \alpha_n) = K(\alpha)$, donde:

$$K(\alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1}) = K(\alpha, \alpha_{n+1})$$

Como sabemos que o resultado vale para o caso com 2 termos, temos que existe $\gamma \in \mathbb{C}$ algébrico sobre K tal que:

$$K(\alpha_1, \alpha_2, ..., \alpha_n, \alpha_{n+1}) = K(\alpha, \alpha_{n+1}) = K(\gamma)$$

Por indução, o resultado segue. □

Por fim, mostremos que $K(\alpha)$ é algébrico sobre K e que o grau de qualquer elemento dessa extensão sobre K não supera o de α. Em particular, este resultado implica que elementos de $\mathbb{C}$ com grau sobre K maiores que o de α não pertencem a $K(\alpha)$.

Teorema 65. *Sejam $K(subcorpo) \subset \mathbb{C}$ e $\alpha \in \mathbb{C}$ algébrico sobre K. Então todo elemento $\beta \in K(\alpha)$ é algébrico sobre K, e o grau de β sobre K é menor ou igual ao grau de α sobre K.*

Demonstração. Sejam $\beta \in K(\alpha)$, com α algébrico sobre K e $n = deg(irr_k(\alpha))$. Pelo Teorema 63 cada uma das potências β^j, com $j = 0, 1, ..., n$ podem ser escritas da forma:

$$\beta^j = \sum_{k=0}^{n-1} a_{jk}\alpha^k$$

com $a_{jk} \in K$. Considere o sistema homogêneo:

$$\sum_{j=0}^{n} a_{jk}x_j = 0, k = 0, 1, ..., n-1$$

Este sistema possui uma solução $(x_0, x_1, ..., x_n) \in K^{n+1}$ não nula, uma vez que o número de incógnitas é maior que o número de equações. Então:

$$\sum_{j=0}^{n} x_j\beta^j = \sum_{j=0}^{n} x_j \sum_{k=0}^{n-1} a_{jk}\alpha^k = \sum_{k=0}^{n-1} \alpha^k \sum_{j=0}^{n} a_{jk}x_j = 0$$

donde β é algébrico sobre K e o grau de β sobre K é menor ou igual que o grau de α sobre K. □

5 CORPOS DE NÚMEROS ALGÉBRICOS

Estudaremos agora corpos de números algébricos, pois, como vimos no Teorema 62, estes estão associados aos domínios $\mathbb{Z}+\mathbb{Z}\sqrt{m}$ e $\mathbb{Z}+\mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right)$, os quais são bastante úteis na resolução de equações diofantinas (em particular, nas equações diofantinas envolvendo termos quadráticos).

5.1 CORPOS DE NÚMEROS ALGÉBRICOS

Definição 51 (Corpo de números algébricos)**.** *Um corpo de números algébricos é um subcorpo de $\mathbb{C}$ da forma $\mathbb{Q}(\alpha_1, ..., \alpha_n)$, em que $\alpha_1, ..., \alpha_n$ são números algébricos.*

Note que, utilizando o Corolário 6, chegamos ao seguinte resultado:

Proposição 18. *Se K é um corpo de números algébricos então existe um número algébrico θ tal que $K = \mathbb{Q}(\theta)$.*

Este resultado, entretanto, pode ser melhorado, como veremos a seguir.

Teorema 66. *Se K é um corpo de números algébricos então existe um inteiro algébrico θ tal que $K = \mathbb{Q}(\theta)$.*

Demonstração. Seja K um corpo de números algébricos. Pela Proposição 18, existe ϕ número algébrico tal que $K = \mathbb{Q}(\phi)$. Pelo Teorema 56, temos $\phi = \frac{\theta}{b}$, em que θ é um inteiro algébrico e $b \in \mathbb{Z} \setminus \{0\}$. Assim, utilizando o Lema 7, temos: $K = \mathbb{Q}(\phi) = \mathbb{Q}\left(\frac{\theta}{b}\right) = \mathbb{Q}(\theta)$. □

Com o resultado anterior, vemos que qualquer corpo de números algébricos é da forma $\{a + b\theta \mid a, b \in \mathbb{Q}\}$, sendo $\theta \in \Omega$. Esta caracterização dos elementos destes corpos terá muitas consequências importantes, inclusive para os inteiros algébricos destes corpos. Em particular, aplicando o Teorema 63 a corpos de números algébricos, temos:

Proposição 19. *Sejam $K = \mathbb{Q}(\theta)$ um corpo de números algébricos, em que θ é um inteiro algébrico e $n = deg(irr_{\mathbb{Q}}(\theta))$. Então todo elemento de K é expresso unicamente da forma:*

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

em que $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$. Ainda, se $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$, temos $c_0+c_1\theta+...+c_{n-1}\theta^{n-1} \in K$.

Segue que K é um espaço vetorial n dimensional sobre $\mathbb{Q}$.

Como discutimos no início deste capítulo, o Teorema 62 nos mostra que o conjunto dos inteiros algébricos de um corpo de números algébricos é um conjunto importante. Estabeleceremos então uma notação para este conjunto e, em seguida, usaremos dos resultados mostrados para extensões de corpos para estudar as propriedades destes conjuntos.

Definição 52 (O conjunto O_K)**.** *O conjunto de todos os inteiros algébricos em um corpo K de números algébricos é denotado por O_K. Isto é:*

$$O_K = \Omega \cap K$$

Teorema 67. *Seja K um corpo de números algébricos. Então O_K é um domínio de integridade.*

Demonstração. Pelo Corolário 5 sabemos que $\Omega \subset \mathbb{C}$ é um domínio de integridade. Como $K \subset \mathbb{C}$ é um corpo, temos $O_K = K \cap \Omega$ domínio de integridade. □

O teorema anterior nos permite renomear o conjunto O_K da seguinte forma:

Definição 53 (Anel de inteiros de um corpo de números algébricos)**.** *O_K é chamado de anel de inteiros do corpo de números algébricos K.*

Teorema 68. *Se K é um corpo de números algébricos então é o corpo quociente de O_K.*

Demonstração. Sejam F o corpo quociente de O_K e $\alpha \in F$. Então $\alpha = \dfrac{b}{c}$, com $b, c \in O_K$ e $c \neq 0$. Como $O_K \subset K$, temos $b, c \in K(corpo)$, com $c \neq 0 \Rightarrow b, c^{-1} \in K \Rightarrow bc^{-1} = \dfrac{b}{c} = \alpha \in K$. Assim, segue que $F \subset K$.

Seja $a \in K$. Como K é corpo de números algébricos, pelo Teorema 56 temos $a = \dfrac{d}{e}$, com d inteiro algébrico e $e \in \mathbb{Z} \setminus \{0\}$. Pelo Lema 9, temos $e \in K$ e, como e é inteiro algébrico, segue que $e \in O_K$. Consequentemente, $ae = d \in K$, donde $d \in O_K$ e, portanto, $a = \dfrac{d}{e} \in F$. Logo, $K \subset F$. Portanto, $K = F$. □

Teorema 69. *Se K é um corpo de números algébricos então O_K é inteiramente fechado.*

Demonstração. Pelo Teorema 68, o corpo quociente de O_K é K. Seja $\beta \in K$ inteiro sobre O_K. Como O_K é inteiro sobre $\mathbb{Z}$, pelo Teorema 53 temos β inteiro sobre $\mathbb{Z}$, donde β é inteiro algébrico. Logo, $\beta \in K \cap \Omega = O_K$ e, portanto, O_K é inteiramente fechado. □

Teorema 70. *Seja K um corpo de números algébricos. Então todo ideal não nulo de O_K contém um inteiro não nulo.*

Demonstração. Sejam $I \neq \langle 0 \rangle$ um ideal de O_K e $\alpha \in I \setminus \{0\}$. Como $\alpha \in I \subset O_K$, temos α inteiro algébrico. Seja $irr_{\mathbb{Q}}(\alpha) = x^n + b_1 x^{n-1} + ... + b_n$. Afirmo que $b_n \neq 0$. De fato, se $n = 1$, $b_n = b_1 = 0$ implicaria em $irr_{\mathbb{Q}}(\alpha) = x$, donde $irr_{\mathbb{Q}}(\alpha)(\alpha) = \alpha = 0$, o que é

um absurdo. Caso $n \geq 2$ então $b_n = 0$ implicaria em $irr_{\mathbb{Q}}(\alpha)$ redutível em $\mathbb{Q}[x]$, o que contradiz o Teorema 57. Logo, $b_n \neq 0$. Pelo Teorema 60 sabemos que $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x]$, uma vez que α é inteiro algébrico. Portanto, $b_1, ..., b_n \in \mathbb{Z}$. Como $\mathbb{Z} \subset \Omega$ e $\mathbb{Z} \subset \mathbb{Q} \subset K$ (pelo Lema 9), temos $\mathbb{Z} \subset \Omega \cap K = O_K$. Assim, como $-1, b_1, ..., b_n \in O_K$ e $\alpha \in I(ideal)$, segue que $b_n = -\alpha^n - b_1\alpha^{n-1} - ... - b_1\alpha \in I$ e $b_n \in \mathbb{Z} \setminus \{0\}$. □

O próximo resultado nos mostra que qualquer ideal não nulo de um corpo de números algébricos K contém um elemento que, quando adjuntado a $\mathbb{Q}$, gera o corpo K. Este fato será importante quando estivermos estudando fatoração de ideais.

Teorema 71. *Sejam K um corpo de números algébricos e $I \neq \langle 0 \rangle$ um ideal de O_K. Então existe $\gamma \in I$ tal que $K = \mathbb{Q}(\gamma)$.*

Demonstração. Pelo Teorema 66 existe $\theta \in O_K$ tal que $K = \mathbb{Q}(\theta)$. Pelo Teorema 70 existe $c \in \mathbb{Z} \cap I \setminus \{0\}$. Seja $\gamma = c\theta$. Como $\theta \in O_K$ e $c \in I$ temos $\gamma \in I$. Ainda, como $c \in \mathbb{Z} \setminus \{0\}$, segue que $K = \mathbb{Q}(\theta) = \mathbb{Q}(c\theta) = \mathbb{Q}(\gamma)$, pelo Lema 7. □

5.2 CORPOS CONJUGADOS DE UM CORPO DE NÚMEROS ALGÉBRICOS

Estudaremos agora os corpos conjugados de um corpo de números algébricos. Para isso, estudaremos homomorfismos de anéis. Em particular, mostraremos que os corpos gerados pela adjunção de um conjugado de um número algébrico a $\mathbb{Q}$ é isomorfo ao corpo algébrico gerado pela adjunção deste número algébrico a $\mathbb{Q}$.

Definição 54 (Homomorfismo)**.** *Sejam R e R' dois anéis. Uma aplicação $\phi : R \to R'$ é dita um homomorfismo se $\forall\ a, b \in R$:*

1. $\phi(a + b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

Definição 55 (Monomorfismo e isomorfismo)**.** *Sejam R e R' dois anéis. Um homomorfismo $\phi : R \to R'$ é dito um monomorfismo se ϕ for injetiva. Caso ϕ seja bijetiva, então ϕ é dito um isomorfismo e R é dito isomorfo a R'.*

Provemos agora algumas propriedades dos homomorfismos, as quais foram complementadas pelo autor deste texto:

Proposição 20. *Sejam A, B e C anéis e $\phi : A \to B$ e $\mu : B \to C$ homomorfismos. Então:*

1. *$\mu \circ \phi : A \to C$ é homomorfismo.*
2. *Se μ e ϕ são monomorfismos, então $\mu \circ \phi$ é monomorfismo.*
3. *Se μ e ϕ são sobrejetoras, então $\mu \circ \phi$ é sobrejetora.*

4. *Se μ e ϕ são isomorfismos, $\mu \circ \phi$ é isomorfismo.*

5. *Se μ é isomorfismo, então μ^{-1} é isomorfismo.*

6. *A relação $\sim$ definida sobre um conjunto de anéis dada por $A \sim B \Leftrightarrow A$ é isomorfo a B é uma relação de equivalência.*

Demonstração. 1. Como μ e ϕ são aplicações, sabemos que $\mu \circ \phi$ está bem definida. Dados $a, b \in A$, temos:

   - $\mu \circ \phi(a + b) = \mu(\phi(a) + \phi(b)) = \mu(\phi(a)) + \mu(\phi(b)) = \mu \circ \phi(a) + \mu \circ \phi(b)$
   - $\mu \circ \phi(ab) = \mu(\phi(a)\phi(b)) = \mu(\phi(a))\mu(\phi(b)) = (\mu \circ \phi(a))(\mu \circ \phi(b))$

   donde $\mu \circ \phi$ é homomorfismo.

2. Sejam $a, b \in A$ tais que $\mu \circ \phi(a) = \mu \circ \phi(b)$. Como μ é monomorfismo, devemos ter $\phi(a) = \phi(b)$. Como ϕ também é monomorfismo, a igualdade anterior implica em $a = b$. Portanto $\mu \circ \phi$ é injetora, donde é monomorfismo.

3. Seja $c \in C$. Como μ é sobrejetora, existe $b \in B$ tal que $\mu(b) = c$. Como ϕ é também sobrejetora, existe $a \in A$ tal que $b = \phi(a)$. Portanto:

$$\mu \circ \phi(a) = \mu(\phi(a)) = \mu(b) = c$$

   donde $\mu \circ \phi$ é sobrejetora.

4. Se μ, ϕ são isomorfismos, então μ, ϕ são monomorfismos sobrejetores. Por 2. e 3., segue que $\mu \circ \phi$ é monomorfismo sobrejetor e, portanto, um isomorfismo.

5. Sabemos que μ^{-1} está bem definido pois μ é bijeção. Dados $c, d \in C$, existem $a, b \in B$ tais que $c = \mu(a)$ e $d = \mu(b)$. Assim:

   - $\mu^{-1}(c + d) = \mu^{-1}(\mu(a) + \mu(b)) = \mu^{-1}(\mu(a + b)) = a + b = \mu^{-1}(c) + \mu^{-1}(d)$
   - $\mu^{-1}(cd) = \mu^{-1}(\mu(a)\mu(b)) = \mu^{-1}(\mu(ab)) = ab = \mu^{-1}(c)\mu^{-1}(d)$

   donde segue que μ^{-1} é homomorfismo. Como μ é bijeção, temos μ^{-1} bijeção, logo μ^{-1} é isomorfismo.

6. Sejam $\mathcal{C}$ um conjunto de anéis, $M, N, P \in \mathcal{C}$ e $\sim \subset \mathcal{C} \times \mathcal{C}$ uma relação dada por $M \sim N \Leftrightarrow M$ é isomorfo a N. Temos:

   - $M \sim M$: Seja $I : M \to M$ a aplicação identidade. Então I é bijetora e, dados $a, b \in M$:

$$I(a + b) = a + b = I(a) + I(b)$$
$$I(ab) = ab = I(a)I(b)$$

     donde I é isomorfismo e $M \sim M$.

- $M \sim N \Rightarrow N \sim M$: Como M é isomorfo a N, existe $\sigma : M \to N$ isomorfismo. Por 5. sabemos que $\sigma^{-1} : N \to M$ é um isomorfismo, donde N é isomorfo a M, ou seja, $N \sim M$.
- $M \sim N$ e $N \sim P \Rightarrow M \sim P$: Como $M \sim N$ e $N \sim P$, existem isomorfismos $\sigma : M \to N$ e $\lambda : N \to P$. Por 4., $\lambda \circ \sigma : M \to P$ é um isomorfismo, donde $M \sim P$.

Portanto, $\sim$ é uma relação de equivalência em $\mathcal{C}$.

□

Lema 10. *Seja $\sigma : K \to K'$ um homomorfismo entre subcorpos de $\mathbb{C}$, tal que $\sigma \neq 0$ (isto é, existe $a \in K$ tal que $\sigma(a) \neq 0$). Então $\sigma(q) = q$ para $q \in \mathbb{Q}$ e, dado $p(x) \in \mathbb{Q}[x]$, temos $\sigma(p(x)) = p(\sigma(x))$.*

Demonstração. Notemos que $\mathbb{Q} \subset K \cap K'$ pelo Lema 9. Primeiramente, mostremos que $\sigma(1) = 1$. De fato:

$$\sigma(1) = \sigma(1 * 1) = \sigma(1)\sigma(1) = \sigma(1)^2 \Rightarrow \sigma(1)^2 - \sigma(1) = 0$$

donde $\sigma(1) \in K' \subset \mathbb{C}$ é uma raiz complexa de $q(x) = x^2 - x = x(x-1) \in \mathbb{C}[x]$. Logo, devemos ter $\sigma(1) = 0$ ou $\sigma(1) = 1$. Suponha que $\sigma(1) = 0$. Dado $a \in K$, temos $\sigma(a) = \sigma(a * 1) = \sigma(a)\sigma(1) = 0$, donde $\sigma = 0$, o que é um absurdo. Logo, $\sigma(1) = 1$. Suponha que $\sigma(n) = n$ para algum $n \in \mathbb{N}$. Então:

$$\sigma(n+1) = \sigma(n) + \sigma(1) = n + 1$$

Pelo princípio de indução, segue que $\sigma(n) = n \ \forall \ n \in \mathbb{N}$. Mostremos agora que $\sigma(-1) = -1$. Temos:

$$1 = \sigma(1) = \sigma(2-1) = \sigma(2) + \sigma(-1) = 2 + \sigma(-1) \Rightarrow \sigma(-1) = -1$$

Consequentemente, $\sigma(0) = \sigma(1-1) = \sigma(1) + \sigma(-1) = 1 - 1 = 0$. Logo, dado $n \in \mathbb{N}$, segue:

$$\sigma(-n) = \sigma(-1 * n) = \sigma(-1) * \sigma(n) = -n$$

Dessa forma, $\sigma(z) = z \ \forall \ z \in \mathbb{Z}$. Resta mostrar agora que $\sigma(a) = a \ \forall \ a \in \mathbb{Q}$. Seja $a \in \mathbb{Q}$. Então existem $p, q \in \mathbb{Z}$, com $q \neq 0$, tais que $a = pq^{-1}$. Logo:

$$\sigma(a)q = \sigma(a)\sigma(q) = \sigma(aq) = \sigma(pq^{-1}q) = \sigma(p) = p \Rightarrow \sigma(a) = \frac{p}{q} = a$$

Portanto, $\sigma \mid_{\mathbb{Q}} = I$. Com isso, sejam $p(x) \in \mathbb{Q}[x]$ e $k \in K$. Existem $a_0, a_1, ..., a_n \in \mathbb{Q}$ tais que:

$$p(x) = a_0 + a_1 x + ... + a_n x^n$$

Assim:

$$\sigma(p(k)) = \sigma(a_0 + a_1k + ... + a_nk^n) = \sigma(a_0) + \sigma(a_1)\sigma(k) + ... + \sigma(a_n)\sigma(k)^n$$
$$= a_0 + a_1\sigma(k) + ... + a_n\sigma(k)^n = p(\sigma(k))$$

donde segue que $p(\sigma(x)) = \sigma(p(x))$. □

Teorema 72. *Seja K um corpo de números algébricos de grau n sobre $\mathbb{Q}$. Então existem exatamente n monomorfismos distintos $\sigma_k : K \to \mathbb{C} (k = 1, ..., n)$.*

Demonstração. Pelo Teorema 18 existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$. Seja $p(x) = irr_{\mathbb{Q}}(\theta)$. Então:

$$deg(p(x)) = deg(irr_{\mathbb{Q}}(\theta)) = [\mathbb{Q}(\theta) : \mathbb{Q}] = n$$

então θ tem n conjugados distintos sobre $\mathbb{Q}$ pelo Teorema 58. Sejam $\theta = \theta_1, \theta_2, ..., \theta_n$ esses conjugados. Então:

$$p(x) = (x - \theta_1)(x - \theta_2)...(x - \theta_n)$$

Pelo Teorema 19 cada elemento $\alpha \in K$ pode ser expresso unicamente na forma $\alpha = a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}$, em que $a_0, a_1, ..., a_{n-1} \in \mathbb{Q}$. Assim, para $k \in \{1, 2, ..., n\}$ podemos definir $\sigma_k : K \to \mathbb{C}$ dado por:

$$\sigma_k(a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}) = a_0 + a_1\theta_k + ... + a_{n-1}\theta_k^{n-1}$$

Começaremos mostrando que $\sigma_k(k = 1, ..., n)$ é um homomorfismo entre corpos. Dados $k \in \{1, ..., n\}$ e $\alpha, \beta \in K$, temos:

$$\alpha = a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}$$
$$\beta = b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1}$$

com $a_0, a_1, ..., a_{n-1}, b_0, b_1, ..., b_{n-1} \in \mathbb{Q}$. Então:

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\theta + ... + (a_{n-1} + b_{n-1})\theta^{n-1}$$
$$\sigma_k(\alpha + \beta) = (a_0 + b_0) + (a_1 + b_1)\theta_k + ... + (a_{n-1} + b_{n-1})\theta_k^{n-1}$$
$$= (a_0 + a_1\theta_k + ... + a_{n-1}\theta_k^{n-1}) + (b_0 + b_1\theta_k + ... + b_{n-1}\theta_k^{n-1})$$
$$= \sigma_k(\alpha) + \sigma_k(\beta)$$

Assim, σ_k é aditivo. Ainda, sejam:

$$f(x) = a_0 + a_1x + ... + a_{n-1}x^{n-1} \in \mathbb{Q}[x]$$
$$g(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1} \in \mathbb{Q}[x]$$

de forma que $f(\theta) = \alpha$ e $g(\theta) = \beta$. Dividindo $f(x)g(x)$ por $p(x)$ em $\mathbb{Q}[x]$, obtemos $q(x), r(x) \in \mathbb{Q}[x]$ tais que:

$$f(x)g(x) = p(x)q(x) + r(x), deg(r(x)) < deg(p(x)) = n$$

Como $deg(r(x)) < n$, existem $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$ tais que:

$$r(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

Assim, e usando o fato de que $p(\theta), p(\theta_k) = 0$, temos:

$$\begin{aligned}\sigma_k(\alpha\beta) &= \sigma_k(f(\theta)g(\theta)) = \sigma_k(p(\theta)q(\theta) + r(\theta)) = \sigma_k(r(\theta)) = \sigma_k(c_0 + c_1\theta + ... + c_{n-1}\theta^{n-1}) \\ &= c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1} = r(\theta_k) = p(\theta_k)q(\theta_k) + r(\theta_k) = f(\theta_k)g(\theta_k) \\ &= (a_0 + a_1\theta_k + ... + a_{n-1}\theta_k^{n-1})(b_0 + b_1\theta_k + ... + b_{n-1}\theta_k^{n-1}) \\ &= \sigma_k(a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1})\sigma_k(b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1}) = \sigma_k(\alpha)\sigma_k(\beta)\end{aligned}$$

donde σ_k é multiplicativo. Logo, σ_k é homomorfismo. Vamos agora mostrar a injetividade. Suponha que $\sigma_k(\alpha) = \sigma_k(\beta)$. Então:

$$a_0 + a_1\theta_k + ... + a_{n-1}\theta_k^{n-1} = b_0 + b_1\theta_k + ... + b_{n-1}\theta_k^{n-1}$$

de forma que θ_k é raiz do polinômio:

$$h(x) = (a_0 - b_0) + (a_1 - b_1)x + ... + (a_{n-1} - b_{n-1})x^{n-1} \in \mathbb{Q}[x]$$

de grau menor que n. Como θ_k é raiz de $p(x) \in \mathbb{Q}[x]$ e $p(x)$ é irredutível em $\mathbb{Q}[x]$, temos $irr_{\mathbb{Q}}(\theta_k) = p(x)$, assim $deg(irr_{\mathbb{Q}}(\theta_k)) = n$. Uma vez que $deg(h(x)) < n$, devemos ter $h(x) = 0$, donde $a_0 = b_0, a_1 = b_1, ..., a_{n-1} = b_{n-1}$ e $\alpha = \beta$. Portanto, σ_k é monomorfismo para $k \in \{1, ..., n\}$.

Por fim, devemos mostrar que estes são os únicos monomorfismos. Seja $\lambda : K \to \mathbb{C}$ um monomorfismo. Então:

$$p(\lambda(\theta)) = \lambda(p(\theta)) = \lambda(0) = 0$$

pelo Lema 10. Consequentemente, existe $k \in \{1, ..., n\}$ tal que $\lambda(\theta) = \theta_k$. Assim, dado $d \in K$, existem $d_0, d_1, ..., d_{n-1} \in \mathbb{Q}$ tais que:

$$d = d_0 + d_1\theta + ... + d_{n-1}\theta^{n-1}$$

de forma que:

$$\begin{aligned}\lambda(d) = \lambda(d_0 + d_1\theta + ... + d_{n-1}\theta^{n-1}) = d_0 + d_1\theta_k + ... + d_{n-1}\theta_k^{n-1} \\ = d_0 + d_1\sigma_k(\theta) + ... + d_{n-1}\sigma_k(\theta^{n-1}) = \sigma_k(d_0 + d_1\theta + ... + d_{n-1}\theta^{n-1}) = \sigma_k(d)\end{aligned}$$

donde $\lambda = \sigma_k$.

Portanto, $\{\sigma_k \mid k = 1, 2, ..., n\}$ são todos os monomorfismos de K em $\mathbb{C}$. □

Com este resultado, podemos provar o seguinte corolário.

Corolário 7. *Sejam K um corpo de números algébricos de grau n sobre $\mathbb{Q}$ e θ um número algébrico tal que $K = \mathbb{Q}(\theta)$. Sejam $\theta_1 = \theta, \theta_2, ..., \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Então os corpos $\mathbb{Q}(\theta_k)$, com $k \in \{1, ..., k\}$ são isomorfos.*

Demonstração. Como $[K : \mathbb{Q}] = n$ e $K = \mathbb{Q}(\theta)$, todo elemento $a \in K$ é escrito de maneira única como sendo $a = a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}$, e todo número desta forma pertence a K, como diz a Proposição 19. Pela demonstração do teorema anterior, sabemos que $\sigma_k : K \to \mathbb{C}$ dado por:

$$\sigma_k(a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1}) = a_0 + a_1\theta_k + ... + a_{n-1}\theta_k^{n-1}$$

é um monomorfismo para $k \in \{1, ..., n\}$. Dado $a = a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1} \in K$, note que $\sigma_k(a) = a_0 + a_1\theta_k + ... + a_{n-1}\theta_k^{n-1} \in \mathbb{Q}(\theta_k)$, de forma que podemos restringir o contradomínio de cada σ_k. Isto é:

$$\begin{aligned} \lambda_k : & K \to \mathbb{Q}(\theta_k) \\ & a \mapsto \sigma_k(a) \end{aligned}$$

é um monomorfismo para $k \in \{1, ..., n\}$. Dados $k \in \{1, ..., n\}$ e $b \in \mathbb{Q}(\theta_k)$, temos que existem $b_0, b_1, ..., b_{n-1} \in \mathbb{Q}$ tais que:

$$b = b_0 + b_1\theta_k + ... + b_{n-1}\theta_k^{n-1}$$

Seja $a = b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1} \in K$. Então:

$$\lambda_k(a) = \lambda_k(b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1}) = \sigma_k(b_0 + b_1\theta + ... + b_{n-1}\theta^{n-1}) = b_0 + b_1\theta_k + ... + b_{n-1}\theta_k^{n-1} = b$$

donde λ_k é sobrejetora e, consequentemente, um isomorfismo entre K e $\mathbb{Q}(\theta_k)$. Como a relação de ser isomorfo é uma relação de equivalência pela Proposição 20 e $K = \mathbb{Q}(\theta_1)$, temos $\mathbb{Q}(\theta_k)$ com $k \in \{1, ..., n\}$ isomorfos entre si. □

O corolário anterior nos leva a seguinte definição:

Definição 56 (Corpos conjugados de um corpo de números algébricos)**.** *Sejam K um corpo de números algébricos, θ um número algébrico tal que $K = \mathbb{Q}(\theta)$ e $\theta_1 = \theta, \theta_2, ..., \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Então os corpos:*

$$\mathbb{Q}(\theta_1) = K, \mathbb{Q}(\theta_2), ..., \mathbb{Q}(\theta_n)$$

são chamados de corpos conjugados de K.

Como a escolha de θ na definição acima não é única, os conjugados $\theta_1, ..., \theta_n$ também não são. Portanto, não é evidente que os corpos conjugados de K sejam independentes da escolha de θ. Tal fato, entretanto, é verdade, como mostra o próximo teorema, o qual faz uso de um importante resultado sobre polinômios simétricos, cujo enunciado, retirado de $(3, Teorema\ III.4.4)$, apresentaremos antes do teorema, sem demonstração.

Teorema 73 (Teorema de Newton)**.** *Seja A um anel e seja $f(X_1, ..., X_n) \in A[X_1, ..., X_n]$ um polinômio simétrico. Então existe um único polinômio $h(X_1, ..., X_n) \in A[X_1, ..., X_n]$, efetivamente calculável, tal que $f(X_1, ..., X_n) = h(s_1, s_2, ..., s_n)$, sendo:*

$$\begin{aligned} s_1 &= X_1 + X_2 + ... + X_n \\ s_2 &= \sum_{1 \leq i_1 < i_2 \leq n} X_{i_1} X_{i_2} \\ &\vdots \\ s_j &= \sum_{1 \leq i_1 < i_2 < ... < i_j \leq n} X_{i_1} X_{i_2} ... X_{i_j} \\ &\vdots \\ s_n &= X_1 X_2 ... X_n \end{aligned}$$

Os polinômios s_j acima, com $j \in \{1, ..., n\}$, são chamados de polinômios simétricos elementares. Vale mencionar que este teorema será usado em mais demonstrações ao longo deste capítulo.

Teorema 74. *Sejam K um corpo de números algébricos, θ um número algébrico tal que $K = \mathbb{Q}(\theta)$ e $\theta_1 = \theta, \theta_2, ..., \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Sejam ϕ outro número algébrico tal que $K = \mathbb{Q}(\phi)$ e $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$ tais que:*

$$\phi = c_0 + c_1\theta + ... + c_{n-1}\theta^{n-1}$$

Para $k \in \{1, ..., n\}$, seja:

$$\phi_k = c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1}$$

de forma que $\phi_1 = \phi$. Então $\phi_1, ..., \phi_n$ são os conjugados de ϕ sobre $\mathbb{Q}$ e:

$$\mathbb{Q}(\theta_k) = \mathbb{Q}(\phi_k), k = 1, ..., n$$

Demonstração. Seja:

$$f(x) = \prod_{k=1}^{n} (x - \phi_k) = \prod_{k=1}^{n} (x - (c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1})) \in K_1[x]$$

com $K_1 = \mathbb{Q}(\theta_1, \theta_2, ..., \theta_n)$.

Pelo Lema 9, temos $\mathbb{Q} \subset K \subset K_1 \subset \mathbb{C}$. Afirmo que $f(x) \in \mathbb{Q}[x]$. De fato, os coeficientes de $f(x)$ são os polinômios simétricos elementares (multiplicados por -1 em alguns termos) em $\phi_k = c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1}$ com $k = 1, ..., n$, e portanto são polinômios com coeficientes racionais sobre os polinômios simétricos elementares em $\theta_1, \theta_2, ..., \theta_n$. Como $\theta_1 + \theta_2 + ... + \theta_n, \theta_1\theta_2 + ... + \theta_{n-1}\theta_n, ..., \theta_1\theta_2...\theta_n$ são racionais (pois são os coeficientes de $irr_{\mathbb{Q}}(\theta) \in \mathbb{Q}[x]$ exceto pelo sinal), temos que os coeficientes de $f(x)$ são racionais. Logo,

$f(x) \in \mathbb{Q}[x]$ e, como $f(\phi) = 0$, temos $irr_{\mathbb{Q}}(\phi) \mid f(x)$, donde $f(x) = irr_{\mathbb{Q}}(\phi)g(x)$ com $g(x) \in \mathbb{Q}[x]$. Então:

$$n = deg(f(x)) = deg(irr_{\mathbb{Q}}(\phi)g(x)) = deg(irr_{\mathbb{Q}}(\phi)) + deg(g(x))$$

Como $deg(irr_{\mathbb{Q}}(\phi)) = [\mathbb{Q}(\phi) : \mathbb{Q}] = [K : \mathbb{Q}] = n$, devemos ter $deg(g(x)) = 0$, donde $g(x) = c \in \mathbb{Q}$ e $f(x) = c\ irr_{\mathbb{Q}}(\phi)$. Uma vez que $f(x)$ e $irr_{\mathbb{Q}}(\phi)$ são mônicos, devemos ter $c = 1$ e, portanto, $f(x) = irr_{\mathbb{Q}}(\phi)$. Dessa forma, $\phi_1, \phi_2, ..., \phi_n$ são os conjugados de ϕ sobre $\mathbb{Q}$. Por fim, dado $k \in \{1, ..., n\}$, temos:

$$\phi_k = c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1} \in \mathbb{Q}(\theta_k) \Rightarrow \mathbb{Q}(\phi_k) \subset \mathbb{Q}(\theta_k)$$

Ainda:

$$n = [\mathbb{Q}(\theta_k) : \mathbb{Q}] = [\mathbb{Q}(\theta_k) : \mathbb{Q}(\phi_k)][\mathbb{Q}(\phi_k) : \mathbb{Q}] = [\mathbb{Q}(\theta_k) : \mathbb{Q}(\phi_k)]n$$
$$\Rightarrow [\mathbb{Q}(\theta_k) : \mathbb{Q}(\phi_k)] = 1$$

donde segue que:

$$\mathbb{Q}(\theta_k) = \mathbb{Q}(\phi_k)\ \forall\ k \in \{1, ..., n\}$$

□

5.3 POLINÔMIO DO CORPO DE UM ELEMENTO DE UM CORPO DE NÚMEROS ALGÉBRICOS

Estudaremos agora um tipo de polinômio que está relacionado com um elemento algébrico sobre $\mathbb{Q}$ e seus conjugados. Veremos que esse polinômio possui diversas propriedades importantes, e que este se conecta com o polinômio irredutível de α.

Sejam K um corpo de números algébricos de grau n sobre $\mathbb{Q}$, $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$ e $\theta_1 = \theta, \theta_2, ..., \theta_n$ os conjugados de θ sobre $\mathbb{Q}$.

Dado $\alpha \in K$ existem únicos $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$ tais que:

$$\alpha = c_0 + c_1\theta + ... + c_{n-1}\theta^{n-1}$$

pela Proposição 19. Para $k \in \{1, ..., n\}$, definamos:

$$\alpha_k = c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1}$$

de forma que $\alpha_1 = \alpha$. Com esta notação, temos a seguinte definição:

Definição 57 (Conjunto completo de conjugados de α relativos a K)**.** *O conjunto de números algébricos $\{\alpha_1 = \alpha, \alpha_2, ..., \alpha_n\}$ é chamado de um conjunto completo de conjugados de α relativos a K. Tal conjunto também pode ser chamado de K-conjugados de α ou conjugados de α relativos a K.*

Vale notar que os conjugados de α relativos a K são obtidos aplicando os monomorfismos $\sigma_k : K \to \mathbb{C}$, com $k \in \{1, ..., n\}$, em α, isto é, $\sigma_k(\alpha) = \alpha_k \in \mathbb{Q}(\theta_k)$.

Podemos agora definir

Definição 58 (Polinômio do corpo de α sobre K)**.** *Sejam K um corpo de números algébricos de grau n sobre $\mathbb{Q}$, $\alpha \in K$ e $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ os K-conjugados de α. Então o polinômio do corpo de α sobre K é o polinômio:*

$$fld_K(\alpha) = \prod_{k=1}^{n}(x - \alpha_k) \in \mathbb{C}[x]$$

Provaremos então propriedades deste polinômio.

Teorema 75. *Sejam K um corpo de números algébricos de grau n e $\alpha \in K$. Então:*

$$fld_K(\alpha) \in \mathbb{Q}[x]$$

Demonstração. Seja $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$. Temos $deg(irr_{\mathbb{Q}}(\theta)) = [\mathbb{Q}(\theta) : \mathbb{Q}] = [K : \mathbb{Q}] = n$. Como $\alpha \in K$, pelo Teorema 19 existem $c_0, c_1, ..., c_{n-1} \in \mathbb{Q}$ tais que:

$$\alpha = c_0 + c_1\theta + ... + c_{n-1}\theta^{n-1}$$

Então os K-conjugados de α são:

$$\alpha_k = c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1}, \;\; k \in \{1, ..., n\}$$

O polinômio do corpo de α sobre K é:

$$fld_K(\alpha) = \prod_{k=1}^{n}(x - \alpha_k) = \prod_{k=1}^{n}(x - (c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1}))$$

de forma que $fld_K(\alpha) \in K_1[x] = \mathbb{Q}(\theta_1, ..., \theta_n)$. Os coeficientes de $fld_K(\alpha)$ são os polinômios simétricos elementares (multiplicados por -1 em alguns termos) em $c_0 + c_1\theta_k + ... + c_{n-1}\theta_k^{n-1}$ com $k = 1, ..., n$, e portanto são polinômios com coeficientes racionais sobre os polinômios simétricos elementares em $\theta_1, \theta_2, ..., \theta_n$. Como $\theta_1 + \theta_2 + ... + \theta_n, \theta_1\theta_2 + ... + \theta_{n-1}\theta_n, ..., \theta_1\theta_2...\theta_n$ são racionais (pois são os coeficientes de $irr_{\mathbb{Q}}(\theta) \in \mathbb{Q}[x]$ exceto pelo sinal), temos que os coeficientes de $fld_K(\alpha)$ são racionais, isto é, $fld_K(\alpha) \in \mathbb{Q}[x]$. □

Teorema 76. *Sejam K um corpo de números algébricos de grau n e $\alpha \in K$. Então:*

$$fld_K(\alpha) = (irr_{\mathbb{Q}}(\alpha))^s$$

em que s é o inteiro positivo:

$$s = \frac{n}{deg(irr_{\mathbb{Q}}(\alpha))}$$

Demonstração. Seja $\{\alpha_1 = \alpha, \alpha_2, ..., \alpha_n\}$ o conjunto completo de conjugados de α em K. Então:

$$fld_K(\alpha) = \prod_{k=1}^{n}(x - \alpha_k) \in \mathbb{Q}[x]$$

pelo Teorema 75. Como $fld_K(\alpha)$ tem α como uma raiz, temos:

$$irr_{\mathbb{Q}}(\alpha) \mid fld_K(\alpha)$$

em $\mathbb{Q}[x]$. Então, como $\mathbb{Q}[x]$ é um domínio de fatoração única, temos:

$$fld_K(\alpha) = (irr_{\mathbb{Q}}(\alpha))^s h(x)$$

em que $h(x) \in \mathbb{Q}[x]$ é um polinômio mônico não divisível por $irr_{\mathbb{Q}}(\alpha)$ e $s \in \mathbb{N}$. Suponha que $deg(h(x)) > 0$. Então, como cada $(x - \alpha_k)$ é irredutível, devemos ter $h(\alpha_k) = 0$ para algum $k \in \{1, ..., n\}$.

Sejam $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$ e $\theta_1, \theta_2, ..., \theta_n$ os conjugados de θ sobre $\mathbb{Q}$. Como $\alpha \in K$ existe $r(x) = a_0 + a_1x + ... + a_{n-1}x_{n-1} \in \mathbb{Q}[x]$ tal que $r(\theta) = \alpha$. Então $\alpha_j = \sigma_j(\alpha) = \sigma_j(r(\theta)) = r(\sigma_j(\theta)) = r(\theta_j)$ para $j \in \{1, ..., n\}$ pelo Lema 10. Seja $g(x) = h(r(x)) \in \mathbb{Q}[x]$. Então $g(\theta_k) = h(r(\theta_k)) = h(\alpha_k) = 0$, donde $g(x)$ é um múltiplo de $irr_{\mathbb{Q}}(\theta_k) = irr_{\mathbb{Q}}(\theta) \in \mathbb{Q}[x]$. Consequentemente, $g(\theta_j) = 0$ para $j \in \{1, ..., n\}$. Em particular, $g(\theta) = 0$ e, portanto, $h(\alpha) = h(r(\theta)) = g(\theta) = 0$. Assim, $irr_{\mathbb{Q}}(\alpha) \mid h(x)$ em $\mathbb{Q}[x]$, o que é um absurdo.

Dessa forma, $h(x)$ é um polinômio constante. Como $h(x)$ é mônico, devemos ter $h(x) = 1$ e, portanto:

$$fld_K(\alpha) = (irr_{\mathbb{Q}}(\alpha))^s$$

Comparando os graus dos polinômios na equação acima, temos:

$$n = deg(fld_K(\alpha)) = s \ deg(irr_{\mathbb{Q}}(\alpha))$$
$$s = \frac{n}{deg(irr_{\mathbb{Q}}(\alpha))}$$

□

Teorema 77. *Sejam K um corpo de números algébricos e $\alpha \in O_K$. Então os K-conjugados de α são inteiros algébricos.*

Demonstração. Seja $\alpha \in O_K$. Pelo Teorema 60, temos:

$$irr_{\mathbb{Q}}(\alpha) \in \mathbb{Z}[x] \tag{5.1}$$

e pelo Teorema 76:

$$fld_K(\alpha) = (irr_{\mathbb{Q}}(\alpha))^s \in \mathbb{Z}[x]$$

donde o resultado segue. □

Teorema 78. *Sejam K um corpo de números algébricos e $\alpha \in K$. Então os K-conjugados de α são iguais se, e somente se, $\alpha \in \mathbb{Q}$.*

Demonstração. Suponha que $\alpha \in \mathbb{Q}$. Então $\alpha_k = \sigma_k(\alpha) = \alpha$ para $k \in \{1, ..., n\}$, donde todos os K-conjugados de α são iguais. Por outro lado, se todos os K-conjugados de α são iguais, temos:

$$fld_K(\alpha) = (x - \alpha)^n$$

Portanto, pelo Teorema 76, segue que:

$$(irr_{\mathbb{Q}}(\alpha))^s = (x - \alpha)^n$$

Mas, pelo Teorema 58, sabemos que as raízes de $irr_{\mathbb{Q}}(\alpha)$ são todas distintas, donde:

$$irr_{\mathbb{Q}}(\alpha) = x - \alpha, s = n$$

Como $irr_{\mathbb{Q}}(\alpha) \in \mathbb{Q}[x]$, devemos ter $\alpha \in \mathbb{Q}$. □

Teorema 79. *Sejam K um corpo de números algébricos e $\alpha \in K$. Então todos os K-conjugados de α são distintos se, e somente se, $K = \mathbb{Q}(\alpha)$.*

Demonstração. Se os K-conjugados de α são todos distintos então $fld_K(\alpha)$ é um produto de fatores lineares distintos e, portanto, pelo Teorema 76, temos $s = 1$ e $irr_{\mathbb{Q}}(\alpha) = fld_K(\alpha)$. Assim:

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = deg(irr_{\mathbb{Q}}(\alpha)) = deg(fld_K(\alpha)) = n = [K : \mathbb{Q}]$$

Como $\mathbb{Q}(\alpha) \subset K$, segue que $K = \mathbb{Q}(\alpha)$. Por outro lado, se $K = \mathbb{Q}(\alpha)$, então $deg(irr_{\mathbb{Q}}(\alpha)) = n$, donde $s = 1$ pelo Teorema 60 e $fld_K(\alpha) = irr_{\mathbb{Q}}(\alpha)$. Como as raízes de $irr_{\mathbb{Q}}(\alpha)$ são todas distintas (pelo Teorema 58), temos os K-conjugados de α todos distintos. □

5.4 O DISCRIMINANTE DE UM CONJUNTO DE ELEMENTOS SOBRE UM CORPO DE NÚMEROS ALGÉBRICOS

Definiremos o discriminante, o qual é uma grandeza associada a um conjunto de elementos de um corpo de números algébricos, e mostraremos que ele possui diversas propriedades importantes, como o fato de ser sempre um número racional. Ainda, mostraremos que podemos usar do discriminante para descobrir propriedades dos elementos, como se estes são linearmente independentes.

Definição 59 (Discriminante de n elementos em um corpo de números algébricos de grau n)**.** *Sejam K um corpo de números algébricos de grau n, $w_1, ..., w_n \in K$ e $\sigma_k (k = 1, ..., n)$ os n monomorfismos distintos de K em $\mathbb{C}$. Para $i = 1, ..., n$, sejam:*

$$\omega_i^{(1)} = \sigma_1(\omega_i) = \omega_i, \omega_i^{(2)} = \sigma_2(\omega_i), ..., \omega_i^{(n)} = \sigma_n(\omega_i)$$

os conjugados de ω_i relativos a K. Então o discriminante de $\{\omega_1, ..., \omega_n\}$ é:

$$D(\omega_1, ..., \omega_n) = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2$$

Definição 60 (Discriminante $D(\alpha)$ de um elemento α)**.** *Sejam K um corpo de números algébricos de grau n e $\alpha \in K$. Definimos o discriminante $D(\alpha)$ de α como sendo:*

$$D(\alpha) = D(1, \alpha, \alpha^2, ..., \alpha^{n-1})$$

A definição de discriminante de um elemento se assemelha bastante ao determinante de uma matriz de Vandermonde. De fato, essa proximidade nos será útil.

Definição 61 (Matriz de Vandermonde)**.** *Dados $m, n \in \mathbb{N}$ e $\alpha_1, \alpha_2, ..., \alpha_m \in \mathbb{C}$, uma matriz V de ordem $m \times n$ é dita uma matriz de Vandermonde se cada uma de suas linhas está em progressão geométrica. Isto é, V é uma matriz de Vandermonde se, reordenando os índices nos α_j se necessário, tivermos:*

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_m & \alpha_m^2 & \cdots & \alpha_m^{n-1} \end{bmatrix}$$

Enunciaremos sem provar uma proposição associada às matrizes de Vandermonde.

Proposição 21. *Sejam $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{C}$ e V uma matriz de Vandermonde de ordem n tal que:*

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

Então o determinante de V é dado por:

$$|V| = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

Usando deste fato, podemos encontrar uma expressão explícita para o discriminante de um elemento.

Teorema 80. *Sejam K um corpo de números algébricos de grau n e $\alpha \in K$. Então:*

$$D(\alpha) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

em que $\alpha_1 = \alpha, \alpha_2, ..., \alpha_n$ são os conjugados de α com respeito a K.

Demonstração. Dado $\alpha \in K$, pela Proposição 21, temos:

$$\begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

Portanto:

$$D(\alpha) = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)^2$$

□

Definiremos agora o discriminante de um polinômio, e mostraremos que este se conecta com o polinômio do corpo de um elemento e com o discriminante deste mesmo elemento.

Definição 62 (Discriminante de um polinômio)**.** *Seja* $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in \mathbb{C}[x]$ *em que* $n \in \mathbb{N}$ *e* $a_n \neq 0$*. Sejam* $x_1, ..., x_n \in \mathbb{C}$ *raízes de* $f(x)$*. O discriminante de* $f(x)$ *é dado por:*

$$disc(f(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in \mathbb{C}$$

Teorema 81. *Sejam* K *um corpo de números algébricos de grau* n *e* $\alpha \in K$*. Então:*

$$D(\alpha) = disc(fld_K(\alpha))$$

Demonstração. Sejam $\alpha^{(1)} = \alpha, \alpha^{(2)}, ..., \alpha^{(n)}$ os K conjugados de α. Então as raízes de $fld_K(\alpha)$ são $\alpha^{(1)}, ..., \alpha^{(n)}$. Então, como $fld_K(\alpha)$ é mônico e usando o Teorema 80, temos:

$$disc(fld_K(\alpha)) = \prod_{1 \leq i < j \leq n} (\alpha^{(i)} - \alpha^{(j)})^2 = D(\alpha)$$

□

Seguimos mostrando propriedades do discriminante.

Teorema 82. *Sejam* K *um corpo de números algébricos de grau* n *e* $\alpha \in K$*. Então:*

$$K = \mathbb{Q}(\alpha) \Leftrightarrow D(\alpha) \neq 0$$

Demonstração. Usando os Teoremas 79 e 80, temos:

$$K = \mathbb{Q}(\alpha) \Leftrightarrow \text{os } K\text{-conjugados de } \alpha \text{ são distintos} \Leftrightarrow D(\alpha) \neq 0$$

□

Teorema 83. *Seja K um corpo de números algébricos de grau n.*

1. *Se $\omega_1, ..., \omega_n \in K$, então $D(\omega_1, ..., \omega_n) \in \mathbb{Q}$;*
2. *Se $\omega_1, ..., \omega_n \in O_K$, então $D(\omega_1, ..., \omega_n) \in \mathbb{Z}$;*
3. *Se $\omega_1, ..., \omega_n \in K$, então:*

$$D(\omega_1, ..., \omega_n) \neq 0 \Leftrightarrow \omega_1, ..., \omega_n \text{ são linearmente independentes sobre } \mathbb{Q}$$

Demonstração. 1. Pelo Teorema 18 temos $K = \mathbb{Q}(\theta)$ para algum $\theta \in K$. Então, para $i = 1, 2, ..., n$, segue que:

$$\omega_i = c_{0i} + c_{1i}\theta + ... + c_{(n-1)i}\theta^{n-1}$$

em que $c_{0i}, c_{1i}, ..., c_{(n-1)i} \in \mathbb{Q}$. Então, para $j \in \{1, 2, ..., n\}$, temos:

$$\omega_i^{(j)} = c_{0i} + c_{1i}\theta_j + ... + c_{(n-1)i}\theta_j^{n-1}$$

com $\theta_1 = \theta, \theta_2, ..., \theta_n$ os conjugados de θ sobre $\mathbb{Q}$ e $\omega_i^{(1)}, ..., \omega_i^{(n)}$ os K-conjugados de ω_i para $i \in \{1, 2, ..., n\}$. Note que permutar os conjugados de θ, isto é, fazer $\theta'_b = \theta_a$ e $\theta'_a = \theta_b$ para algum par a, b faz com que:

$$\omega_i^{'(b)} = c_{0i} + c_{1i}\theta'_b + ... + c_{(n-1)i}\theta_b^{'n-1} = c_{0i} + c_{1i}\theta_a + ... + c_{(n-1)i}\theta_a^{n-1} = \omega_i^{(a)}$$
$$\omega_i^{'(a)} = c_{0i} + c_{1i}\theta'_a + ... + c_{(n-1)i}\theta_a^{'n-1} = c_{0i} + c_{1i}\theta_b + ... + c_{(n-1)i}\theta_b^{n-1} = \omega_i^{(b)}$$

de forma que tal processo apenas permuta as linhas da matriz:

$$\begin{bmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{bmatrix}$$

fazendo com que seu determinante não seja alterado. Como qualquer permutação entre os conjugados pode ser obtida através de sucessivas permutações entre dois termos, segue que $D(\omega_1, ..., \omega_n)$ não é alterado. Portanto, $D(\omega_1, ..., \omega_n)$ é uma função simétrica das raízes do polinômio:

$$(x - \theta_1)(x - \theta_2)...(x - \theta_n) = x^n + a_{n-1}x^{n-1} + ... + a_0$$

com $a_0, a_1, ..., a_{n-1} \in \mathbb{Q}$. Pelo Teorema de Newton, $D(\omega_1, ..., \omega_n)$ é um polinômio nos coeficientes $a_0, a_1, ..., a_{n-1}$ e portanto um número racional.

2. Se $\omega_1, ..., \omega_n \in O_K$ então $D(\omega_1, ..., \omega_n) \in O_K$, uma vez que O_K é domínio de integridade e $D(\omega_1, ..., \omega_n)$ é obtido de $\omega_1, ..., \omega_n$ através de uma série de adições e multiplicações destes termos. Como $D(\omega_1, ..., \omega_n) \in \mathbb{Q}$, temos pelo Teorema 16 que $D(\omega_1, ..., \omega_n) \in \mathbb{Z}$.

3. Se o conjunto $\{\omega_1, ..., \omega_n\}$ é linearmente dependente sobre $\mathbb{Q}$, então existem $c_1, ..., c_n \in \mathbb{Q}$ não todos nulos tais que:

$$c_1\omega_1 + ... + c_n\omega_n = 0$$

Aplicando cada monomorfismo σ_k, com $k \in \{1, ..., n\}$, a equação acima, obtemos o seguinte sistema homogêneo de n equações lineares sobre $c_1, ..., c_n$:

$$\begin{cases} c_1\omega_1^{(1)} + ... + c_n\omega_n^{(1)} = 0 \\ c_1\omega_1^{(2)} + ... + c_n\omega_n^{(2)} = 0 \\ \qquad\qquad \vdots \\ c_1\omega_1^{(n)} + ... + c_n\omega_n^{(n)} = 0 \end{cases}$$

Como este sistema tem solução não trivial $(c_1, ..., c_n) \neq (0, ..., 0) \in \mathbb{Q}^n$, devemos ter seu determinante igual a 0, isto é:

$$\begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix} = 0$$

donde:

$$D(\omega_1, ..., \omega_n) = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2 = 0$$

Por outro lado, suponha que $\{\omega_1, ..., \omega_n\}$ é linearmente independente sobre $\mathbb{Q}$. Então $\{\omega_1, ..., \omega_n\}$ é uma base para o espaço vetorial K sobre o corpo $\mathbb{Q}$. Em particular, como $1, \theta, ..., \theta^{n-1} \in K$ existem $c_{ij} \in \mathbb{Q}$ com $i, j \in \{1, ..., n\}$ tais que:

$$\begin{cases} 1 = c_{11}\omega_1 + ... + c_{1n}\omega_n \\ \theta = c_{21}\omega_1 + ... + c_{2n}\omega_n \\ \qquad\qquad \vdots \\ \theta^{n-1} = c_{n1}\omega_1 + ... + c_{nn}\omega_n \end{cases}$$

Então:

$$D(\theta) = D(1, \theta, ..., \theta^{n-1}) = |det(c_{ij})|^2 D(\omega_1, ..., \omega_n)$$

Como $K = \mathbb{Q}(\theta)$, pelo Teorema 82 sabemos que $D(\theta) \neq 0$ donde:

$$D(\omega_1, ..., \omega_n) \neq 0$$

□

Teorema 84. *Sejam K um corpo de números algébricos com $[K:\mathbb{Q}] = n$ e $I \neq \langle 0 \rangle$ um ideal de O_K. Então existem $\nu_1, ..., \nu_n \in I$ tais que:*

$$D(\nu_1, ..., \nu_n) \neq 0$$

Demonstração. Pelo Teorema 66 temos $K = \mathbb{Q}(\theta)$ para algum $\theta \in O_K$. Pelo Teorema 82, temos $D(\theta) \neq 0$. Ainda, pelo Teorema 70, como I é um ideal não nulo de O_K, existe $c \in I \cap \mathbb{Z}$ com $c \neq 0$. Então, como I é ideal de O_K, temos:

$$\nu_1 = c, \nu_2 = c\theta, ..., \nu_n = c\theta^{n-1} \in I$$

e

$$D(\nu_1, ..., \nu_n) = D(c, c\theta, ..., c\theta^{n-1}) = c^{2n} D(1, \theta, ..., \theta^{n-1}) = c^{2n} D(\theta) \neq 0$$

□

Em particular, temos pelos dois resultados anteriores que todo ideal não-nulo de O_K contém n elementos linearmente independentes sobre $\mathbb{Q}$. Tal fato nos servirá para mostrar o próximo teorema, que motivará uma definição mais a frente.

Teorema 85. *Sejam K um corpo de números algébricos de grau n e $I \neq \langle 0 \rangle$ um ideal de O_K. Então existem elementos $\nu_1, ..., \nu_n \in I$ tais que cada elemento $\alpha \in I$ pode ser expresso unicamente na forma:*

$$\alpha = x_1\nu_1 + ... + x_n\nu_n$$

em que $x_1, ..., x_n \in \mathbb{Z}$.

Demonstração. Como I é um ideal não nulo de O_K, pelo Teorema 84 existe um conjunto $\{\nu_1, ..., \nu_n\} \subset I$ tais que $D(\nu_1, ..., \nu_n) \neq 0$. Pelo Teorema 83, $D(\nu_1, ..., \nu_n) \in \mathbb{Z}$ de forma que $|D(\nu_1, ..., \nu_n)| \in \mathbb{N}$. Seja:

$$S = \{|D(\nu_1, ..., \nu_n)| \ \mid \ \nu_1, ..., \nu_n \in I, D(\nu_1, ..., \nu_n) \neq 0\}$$

Como $S \subset \mathbb{N}$ e $S \neq \emptyset$, S possui um elemento mínimo $|D(\nu_1, ..., \nu_n)|$, com $\nu_1, ..., \nu_n \in I$. Como $D(\nu_1, ..., \nu_n) \neq 0$, pelo item 3 do Teorema 83, segue que $\{\nu_1, ..., \nu_n\}$ é uma base para o espaço vetorial K sobre $\mathbb{Q}$. Seja $\alpha \in I$. Então existem únicos $x_1, ..., x_n \in \mathbb{Q}$ tais que:

$$\alpha = x_1\nu_1 + ... + x_n\nu_n$$

Suponha que pelo menos um x_i não é um inteiro. Permutando $\nu_1, ..., \nu_n$, se necessário, podemos supor que $x_1 \notin \mathbb{Z}$. Então existe um único inteiro l tal que:

$$l < x_1 < l + 1$$

Seja $\gamma = \alpha - l\nu_1$. Como $\alpha \in I$ e $\nu_1 \in I$ temos $\gamma \in I$. Note que $\gamma = (x_1 - l)\nu_1 + ... + x_n\nu_n$. Aplicando cada monomorfismo σ_k, com $k \in \{1, 2, ..., n\}$, a γ, temos:

$$\begin{cases} \gamma^{(1)} = (x_1 - l)\nu_1^{(1)} + x_2\nu_2^{(1)}... + x_n\nu_n^{(1)} \\ \gamma^{(2)} = (x_1 - l)\nu_1^{(2)} + x_2\nu_2^{(2)}... + x_n\nu_n^{(2)} \\ \qquad\qquad\qquad \vdots \\ \gamma^{(n)} = (x_1 - l)\nu_1^{(n)} + x_2\nu_2^{(n)}... + x_n\nu_n^{(n)} \end{cases}$$

em que $\gamma = \gamma^{(1)}, \gamma^{(2)}, ..., \gamma^{(n)}$ são os K-conjugados de γ e $\nu_i^{(1)} = \nu_i, \nu_i^{(2)}, ..., \nu_i^{(n)}$ são os K-conjugados de ν_i com $i \in \{1, 2, ..., n\}$. Pela regra de Cramer, deduzimos que:

$$x_1 - l = \frac{\begin{vmatrix} \gamma^{(1)} & \nu_2^{(1)} & \cdots & \nu_n^{(1)} \\ \gamma^{(2)} & \nu_2^{(2)} & \cdots & \nu_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{(n)} & \nu_2^{(n)} & \cdots & \nu_n^{(n)} \end{vmatrix}}{\begin{vmatrix} \nu_1^{(1)} & \nu_2^{(1)} & \cdots & \nu_n^{(1)} \\ \nu_1^{(2)} & \nu_2^{(2)} & \cdots & \nu_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \nu_1^{(n)} & \nu_2^{(n)} & \cdots & \nu_n^{(n)} \end{vmatrix}}$$

Então:

$$(x_1 - l)^2 = \frac{D(\gamma, \nu_2, ..., \nu_n)}{D(\nu_1, \nu_2, ..., \nu_n)}$$

de forma que:

$$0 < |D(\gamma, \nu_2, ..., \nu_n)| = (x_1 - l)^2 |D(\nu_1, \nu_2, ..., \nu_n)| < |D(\nu_1, \nu_2, ..., \nu_n)|$$

Isso contradiz a minimalidade de $|D(\nu_1, \nu_2, ..., \nu_n)|$. Então todos os x_i são inteiros e cada elemento $\alpha \in I$ pode ser expresso unicamente na forma $\alpha = x_1\nu_1 + ... + x_n\nu_n$. □

Como $\nu_1, ..., \nu_n \in I$ e I é um ideal, temos:

$$\mathbb{Z}\nu_1 + ... + \mathbb{Z}\nu_n = \{k_1\nu_1 + ... + k_n\nu_n \mid k_1, ..., k_n \in \mathbb{Z}\} \subset I$$

e o Teorema 85 nos diz que:

$$I \subset \mathbb{Z}\nu_1 + ... + \mathbb{Z}\nu_n$$

donde:

$$I = \mathbb{Z}\nu_1 + ... + \mathbb{Z}\nu_n$$

de forma que I é um $\mathbb{Z}$-módulo finitamente gerado.

Teorema 86. *Seja K um corpo de números algébricos. Então O_K é um domínio Noetheriano.*

Demonstração. Sabemos que $\mathbb{Z}$ e O_K são domínios de integridade com $\mathbb{Z} \subset O_K$ e que $\mathbb{Z}$ é um domínio Noetheriano. Pelo Teorema 85, temos $O_K = \langle 1 \rangle$ é um $\mathbb{Z}$-módulo finitamente gerado. Portanto, pelo Teorema 42, O_K é um domínio Noetheriano. □

Os resultados anteriores nos levam a seguinte definição:

Definição 63 (Base de um ideal)**.** *Sejam K um corpo de números algébricos de grau n e $I \neq \langle 0 \rangle$ um ideal de O_K. Se $\{\nu_1, ..., \nu_n\}$ é um conjunto de elementos de I tal que cada elemento $\alpha \in I$ pode ser expresso unicamente na forma:*

$$\alpha = x_1\nu_1 + ... + x_n\nu_n, \text{ com } x_1, ..., x_n \in \mathbb{Z}$$

então $\{\nu_1, ..., \nu_n\}$ é chamado base para um ideal I.

Como a representação de cada elemento α de um ideal $I \neq \langle 0 \rangle$ por uma base $\{\nu_1, ..., \nu_n\}$ é único, os elementos da base $\nu_1, ..., \nu_n$ são linearmente independentes sobre $\mathbb{Q}$.

Mostremos como o discriminante se relaciona com as bases de um ideal I de O_K.

Teorema 87. *Sejam K um corpo de números algébricos de grau n e $I \neq \langle 0 \rangle$ um ideal de O_K.*

1. *Sejam $\{\nu_1, ..., \nu_n\}$ e $\{\lambda_1, ..., \lambda_n\}$ duas bases para I. Então:*

$$D(\nu_1, ..., \nu_n) = D(\lambda_1, ..., \lambda_n)$$

e

$$\nu_i = \sum_{j=1}^{n} c_{ij}\lambda_j,$$

em que $c_{ij} \in \mathbb{Z}$ para $i, j \in \{1, 2, ..., n\}$ são tais que:

$$\begin{vmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{vmatrix} = \pm 1$$

2. *Sejam $\{\nu_1, ..., \nu_n\}$ uma base para I e $\lambda_1, ..., \lambda_n \in I$ tais que:*

$$D(\lambda_1, ..., \lambda_n) = D(\nu_1, ..., \nu_n)$$

Então $\{\lambda_1, ..., \lambda_n\}$ é uma base para I.

Demonstração. 1. Como $\{\lambda_1, ..., \lambda_n\}$ é uma base para I, temos:

$$I = \mathbb{Z}\lambda_1 + ... + \mathbb{Z}\lambda_n$$

Como $\nu_1, ..., \nu_n \in I$ existem $c_{ij} \in \mathbb{Z}$ com $i, j \in \{1, 2, ..., n\}$ tais que:

$$\nu_i = \sum_{j=1}^{n} c_{ij}\lambda_j,$$

Uma vez que $\{\nu_1, ..., \nu_n\}$ é uma base para I, temos:

$$I = \mathbb{Z}\nu_1 + ... + \mathbb{Z}\nu_n$$

Visto que $\lambda_1, ..., \lambda_n \in I$ existem $d_{jk} \in \mathbb{Z}$ com $j, k \in \{1, 2, ..., n\}$ tais que:

$$\lambda_j = \sum_{k=1}^{n} d_{jk}\nu_k,$$

Então, para $i = 1, 2, ..., n$, temos:

$$\nu_i = \sum_{j=1}^{n} c_{ij} \sum_{k=1}^{n} d_{jk}\nu_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} c_{ij}d_{jk} \right) \nu_k$$

Como $\{\nu_1, ..., \nu_n\}$ é uma base para I, temos que $\nu_1, ..., \nu_n$ são linearmente independentes sobre $\mathbb{Q}$, de forma que:

$$\sum_{j=1}^{n} c_{ij}d_{jk} = \begin{cases} 1, & \text{se } i = k \\ 0, & \text{se } i \neq k \end{cases}$$

Definimos as matrizes $n \times n$ C e D como sendo:

$$C = [c_{ij}], D = [d_{ij}]$$

de forma que C e D tem elementos inteiros. Então:

$$CD = [\sum_{j=1}^{n} c_{ij}d_{jk}] = I_n$$

em que I_n é a matriz identidade de ordem n. Assim:

$$det(C)det(D) = det(CD) = det(I_n) = 1$$

Como $det(C), det(D) \in \mathbb{Z}$, devemos ter:

$$det(C) = det(D) = \pm 1$$

Sabendo que $\nu_i = \sum_{j=1}^{n} c_{ij}\lambda_j$ para $i \in \{1, ..., n\}$, temos:

$$D(\nu_1, ..., \nu_n) = (det(c_{ij}))^2 D(\lambda_1, ..., \lambda_n) = (det(C))^2 D(\lambda_1, ..., \lambda_n)$$

donde:

$$D(\nu_1, ..., \nu_n) = (\pm 1)^2 D(\lambda_1, ..., \lambda_n) = D(\lambda_1, ..., \lambda_n)$$

2. Como $\{\nu_1, ..., \nu_n\}$ é uma base para I e $\lambda_1, ..., \lambda_n \in I$, existem $d_{ij} \in \mathbb{Z}$, com $i, j \in \{1, ..., n\}$, tais que:

$$\lambda_i = \sum_{j=1}^{n} d_{ij}\nu_j,$$

Então:

$$D(\lambda_1, ..., \lambda_n) = (det(d_{ij}))^2 D(\nu_1, ..., \nu_n)$$

Como $D(\lambda_1, ..., \lambda_n) = D(\nu_1, ..., \nu_n)$, deduzimos que:

$$(det(d_{ij}))^2 = 1$$

donde $det(d_{ij}) = \pm 1$. Consequentemente a matriz $D = (d_{ij})$ tem uma inversa $D^{-1} = C = (c_{ij})$ cujos elementos são todos inteiros, e:

$$\nu_i = \sum_{j=1}^{n} c_{ij}\lambda_j, i = 1, 2, ..., n$$

Seja $\alpha \in I$. Então, como $\{\nu_1, ..., \nu_n\}$ é uma base para I, existem $a_1, ..., a_n \in \mathbb{Z}$ tais que:

$$\alpha = \sum_{i=1}^{n} a_i\nu_i$$

Portanto:

$$\alpha = \sum_{i=1}^{n} a_i \sum_{j=1}^{n} c_{ij}\lambda_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} a_i c_{ij} \right) \lambda_j$$

em que cada $\sum_{i=1}^{n} a_i c_{ij} \in \mathbb{Z}$ com $j \in \{1, ..., n\}$. Isto mostra que todo elemento α de I pode ser expresso da forma:

$$\alpha = b_1\lambda_1 + ... + b_n\lambda_n$$

com $b_1, ..., b_n \in \mathbb{Z}$.

Suponha que α pode ser expresso de mais de uma maneira nesta forma, isto é:

$$\alpha = b_1\lambda_1 + ... + b_n\lambda_n = b'_1\lambda_1 + ... + b'_n\lambda_n$$

com $b_1, ..., b_n, b'_1, ..., b'_n \in \mathbb{Z}$. Então:

$$e_1\lambda_1 + ... + e_n\lambda_n = 0$$

com $e_i = b_i - b'_i \in \mathbb{Z}$ para $i \in \{1, 2, ..., n\}$. Se pelo menos um dos e_i é diferente de 0 então $\lambda_1, ..., \lambda_n$ são linearmente dependentes sobre $\mathbb{Q}$ e pelo Teorema 83 item 3. temos:

$$D(\lambda_1, ..., \lambda_n) = 0$$

e portanto:

$$D(\nu_1, ..., \nu_n) = 0$$

de forma que $\nu_1, ..., \nu_n$ é linearmente dependente sobre $\mathbb{Q}$, o que é um absurdo. Logo $e_i = 0$ para $i = 1, 2, ..., n$, donde $b_i = b_i'$ para $i = 1, 2, ..., n$ e α é unicamente expresso na forma $b_1\lambda_1 + ... + b_n\lambda_n$ com $b_1, ..., b_n \in \mathbb{Z}$. Portanto, $\{\lambda_1, ..., \lambda_n\}$ é uma base para I.

□

Se $\{\nu_1, ..., \nu_n\}$ e $\{\lambda_1, ..., \lambda_n\}$ são duas bases para o mesmo ideal não nulo do anel de inteiros de um corpo de números algébricos então sabemos pelo Teorema 87 que:

$$D(\nu_1, ..., \nu_n) = D(\lambda_1, ..., \lambda_n)$$

Assim, podemos apresentar a seguinte definição:

Definição 64 (Discriminante de um ideal)**.** *Sejam K um corpo de números algébricos de grau n, $\langle 0\rangle \neq I \subset O_K$ e $\{\nu_1, ..., \nu_n\}$ uma base de I. Então o discriminante $D(I)$ do ideal I é o inteiro diferente de 0 dado por:*

$$D(I) = D(\nu_1, ..., \nu_n)$$

Teorema 88. *Sejam K um corpo quadrático e $m \in \mathbb{Z}$ o único inteiro livre de quadrados tal que $K = \mathbb{Q}(\sqrt{m})$.*

1. *Caso $m \not\equiv 1 \pmod 4$, sejam $a, b, c \in \mathbb{Z}$ com $a, c \neq 0$. Então:*

$$\{a, b + c\sqrt{m}\} \text{ é uma base para o ideal } \left\langle a, b + c\sqrt{m}\right\rangle$$

se, e somente se,

$$c \mid a,\ \ c \mid b,\ \ ac \mid b^2 - mc^2$$

2. *Caso $m \equiv 1 \pmod 4$, sejam $a, b, c \in \mathbb{Z}$ com $a, c \neq 0$ e $b \equiv c \pmod 2$. Então:*

$$\left\{a, \frac{b + c\sqrt{m}}{2}\right\} \text{ é uma base para o ideal } \left\langle a, \frac{b + c\sqrt{m}}{2}\right\rangle$$

se, e somente se,

$$c \mid a,\ \ c \mid b,\ \ 4ac \mid b^2 - mc^2$$

Demonstração. Provaremos apenas a primeira afirmação, uma vez que a segunda segue de maneira análoga.

1. Suponha que $c \mid a$, $c \mid b$ e $ac \mid b^2 - mc^2$. Então existem $x, y, z \in \mathbb{Z}$ tais que:

$$a = cx,\ \ b = cy,\ \ b^2 - mc^2 = acz$$

Então:

$$bx - ay = 0,\ \ by - az = mc$$

Seja $\alpha \in I = \langle a, b + c\sqrt{m} \rangle$. Existe $\theta \in O_K$ e $\phi \in O_K$ tais que:

$$\alpha = \theta a + \phi(b + c\sqrt{m})$$

Como $\theta, \phi \in O_K$ e $m \not\equiv 1 \pmod 4$, pelo Teorema 62 existem inteiros r, s, t, u tais que:

$$\theta = r + s\sqrt{m}, \;\; \phi = t + u\sqrt{m}$$

Assim:

$$\begin{aligned}
\alpha &= (r + s\sqrt{m})a + (t + u\sqrt{m})(b + c\sqrt{m}) = \\
&= (ra + tb + umc) + (sa + tc + ub)\sqrt{m} = \\
&= s(bx - ay) + (ra + tb + u(by - az)) + (scx + tc + ucy)\sqrt{m} = \\
&= (r - sy - uz)a + (t + sx + uy)(b + c\sqrt{m})
\end{aligned}$$

donde $\{a, b + c\sqrt{m}\}$ é base para I.

Por outro lado, suponha que $\{a, b + c\sqrt{m}\}$ é uma base para $I = \langle a, b + c\sqrt{m} \rangle$. Como $a\sqrt{m} \in I$ e $\sqrt{m}(b + c\sqrt{m}) \in I$ existem inteiros x, y, u, v tais que:

$$\begin{aligned}
a\sqrt{m} &= xa + y(b + c\sqrt{m}) \\
(b + c\sqrt{m})\sqrt{m} &= ua + v(b + c\sqrt{m})
\end{aligned}$$

Igualando os coeficientes de 1 e $\sqrt{m}$, obtemos:

$$\begin{aligned}
xa + yb &= 0 \\
yc &= a \\
ua + vb &= cm \\
vc &= b
\end{aligned}$$

Da segunda e quarta equações, vemos que $c \mid a$ e $c \mid b$, respectivamente. Da terceira e da quarta equações, obtemos:

$$uac + b^2 = c^2 m$$

de forma que:

$$ac \mid b^2 - mc^2$$

□

Teorema 89. *Seja P um ideal primo do anel O_K de inteiros de um corpo de números algébricos K. Então P é um ideal maximal de O_K.*

Demonstração. Suponha que o teorema seja falso. Então existe um ideal primo P_1 de O_K que não é um ideal maximal. Seja $S = \{I \subsetneq O_K \mid I \text{ é ideal de } O_K, P_1 \subsetneq I\}$. Como P_1 não é ideal maximal, temos $S \neq \emptyset$. Pelo Teorema 86, O_K é um domínio Noetheriano. Então, pelo Teorema 36, S contém um elemento maximal. Isto é, existe um ideal maximal P_2 tal que:

$$P_1 \subsetneq P_2 \subsetneq O_K$$

Pelo Teorema 13, sabemos que P_2 é um ideal primo. Como cada ideal não nulo em O_K contém um $z \in \mathbb{Z} \setminus \{0\}$ (pelo Teorema 70), vemos que $P_1 \cap \mathbb{Z} \neq \{0\}$. Então, pelo Teorema 16, $P_1 \cap \mathbb{Z}$ é um ideal primo de $\mathbb{Z}$. Mas $\mathbb{Z}$ é um domínio de ideais principais, de forma que $P_1 \cap \mathbb{Z} = \langle p \rangle$ para algum $p \in \mathbb{Z}$. Pelo Teorema 11, segue que p é primo. Portanto:

$$\langle p \rangle = P_1 \cap \mathbb{Z} \subset P_2 \cap \mathbb{Z} \subset \mathbb{Z}$$

Note que $P_2 \cap \mathbb{Z} \neq \mathbb{Z}$, pois $1 \notin P_2$. Uma vez que $\langle p \rangle$ é ideal maximal de $\mathbb{Z}$ (pelo Teorema 14), temos:

$$P_1 \cap \mathbb{Z} = P_2 \cap \mathbb{Z} = \langle p \rangle$$

Como $P_1 \subset P_2$, existe $\alpha \in P_2 \setminus P_1$. Uma vez que $\alpha \in O_K$, existem $k \in \mathbb{N}$ e $a_0, ..., a_{k-1} \in \mathbb{Z}$ tais que:

$$\alpha^k + a_{k-1}\alpha^{k-1} + ... + a_1\alpha + a_0 = 0 \in P_1$$

Seja l o menor inteiro positivo para o qual existem $b_0, ..., b_{l-1} \in \mathbb{Z}$ tais que:

$$\alpha^l + b_{l-1}\alpha^{l-1} + ... + b_1\alpha + b_0 \in P_1$$

Como $\alpha \in P_2$, temos:

$$\alpha^l + b_{l-1}\alpha^{l-1} + ... + b_1\alpha = \alpha(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + ... + b_1) \in P_2$$

Então, como $P_1 \subset P_2$ e P_2 é um ideal:

$$b_0 = (\alpha^l + b_{l-1}\alpha^{l-1} + ... + b_1\alpha + b_0) - (\alpha^l + b_{l-1}\alpha^{l-1} + ... + b_1\alpha) \in P_2$$

Mas $b_0 \in \mathbb{Z}$, de forma que:

$$b_0 \in P_2 \cap \mathbb{Z} = P_1 \cap \mathbb{Z}$$

donde $b_0 \in P_1$. Do fato de que $\alpha^l + b_{l-1}\alpha^{l-1} + ... + b_1\alpha + b_0 \in P_1$, deduzimos que:

$$\alpha^l + b_{l-1}\alpha^{l-1} + ... + b_1\alpha \in P_1$$

Se $l = 1$, temos $\alpha \in P_1$, o que é um absurdo. Logo, $l \geq 2$, donde:

$$\alpha(\alpha^{l-1} + b_{l-1}\alpha^{l-2} + ... + b_1) \in P_1$$

Como P_1 é um ideal primo e $\alpha \notin P_1$, segue que:

$$\alpha^{l-1} + b_{l-1}\alpha^{l-2} + ... + b_1 \in P_1$$

o que contradiz a minimalidade de l.

Com isso, o resultado segue. □

6 DOMÍNIOS DE DEDEKIND

Neste capítulo, estudaremos os domínios de Dedekind. Um dos motivos por trás do estudo destes domínios se dá pelo fato de nem todo domínio de integridade ser um domínio de fatoração única. De fato, ao estudarmos equações diofantinas na Teoria Elementar dos Números, um método comum e eficaz na resolução destas equações consiste em reescrevermos a equação analisada como um produto de elementos (geralmente, com MDC igual a 1) e utilizarmos do Teorema Fundamental da Aritmética para obtermos informações sobre os termos deste produto e, consequentemente, sobre as possíveis soluções da equação. Para isso, utilizamos fortemente da unicidade no Teorema Fundamental da Aritmética, a qual, como vimos, é perdida se o domínio não é um domínio de fatoração única. Por isso, estudaremos os domínios de Dedekind: com eles, conseguimos restaurar a unicidade da fatoração fatorando os ideais ao invés dos termos da equação, como veremos mais adiante, nos permitindo aplicar um método semelhante ao utilizado na Teoria Elementar dos Números, mesmo em domínios que não são de fatoração única.

6.1 DOMÍNIOS DE DEDEKIND

Vimos no capítulo 5 que o anel de inteiros algébricos O_K de um corpo de números algébricos K tem as seguintes propriedades:

- O_K é um domínio Noetheriano (pelo Teorema 86).
- O_K é inteiramente fechado (pelo Teorema 69).
- Cada ideal primo P de O_K é um ideal maximal (pelo Teorema 89).

Um domínio de integridade que satisfaz essas 3 propriedades é chamado domínio de Dedekind.

Definição 65 (Domínio de Dedekind)**.** *Um domínio de integridade D que satisfaz as propriedades:*

- *D é um domínio Noetheriano.*
- *D é inteiramente fechado.*
- *Cada ideal primo P de D é um ideal maximal.*

é chamado domínio de Dedekind.

Em particular, pelas observações anteriores, segue o seguinte teorema:

Teorema 90. *Sejam K um corpo de números algébricos e O_K seu anel de inteiros. Então O_K é um domínio de Dedekind.*

Mostremos que outro tipo de domínio é também um domínio de Dedekind.

Teorema 91. *Seja D um domínio de ideais principais. Então D é um domínio de Dedekind.*

Demonstração. Seja D um domínio de ideais principais. Pelo Corolário 2, D é um domínio Noetheriano. Pelo Teorema 38, D é um domínio de fatoração única e, portanto, pela Proposição 17, D é inteiramente fechado. Por fim, pela Teorema 14 todo ideal primo de D é maximal. Assim, D é um domínio de Dedekind. □

6.2 IDEAIS EM UM DOMÍNIO DE DEDEKIND

Queremos provar que podemos fatorar ideais unicamente em um domínio de Dedekind como um produto de ideais primos. Para isso, mostremos primeiro que todo ideal não nulo contém um produto de ideais primos.

Teorema 92. *Em um domínio Noetheriano todo ideal não-nulo contém um produto de um ou mais ideais primos.*

Demonstração. Suponha que D é um domínio Noetheriano que possui pelo menos um ideal não-nulo que não contém o produto de um ou mais ideais primos. Seja então $S \neq \emptyset$ o conjunto destes ideais. Como D é Noetheriano, pelo Teorema 36, S contém um ideal não-nulo A tal que A é o elemento maximal de S. Em particular, pela definição de S, A não é um ideal primo. Então, pelo Teorema 15, existem ideais B e C tais que:

$$BC \subset A, B \not\subset A \text{ e } C \not\subset A$$

Definamos ideais B_1 e C_1 de D como sendo:

$$B_1 = A + B \text{ e } C_1 = A + C$$

De forma que:

$$A \subsetneq B_1 \text{ e } A \subsetneq C_1$$

donde $B_1, C_1 \notin S$. Portanto, existem ideais primos $P_1, ..., P_k$ de D tais que:

$$P_1...P_h \subset B_1 \text{ e } P_{h+1}...P_k \subset C_1$$

Entretanto, isso implica em:

$$P_1...P_k \subset B_1C_1 = (A + B)(A + C) = AA + AC + BA + BC \subset A$$

pois $BC \subset A$ por hipótese e $AA, AC, BA \subset A$ pelas propriedades do produto de ideais. Tal fato é um absurdo, pois contradiz $A \in S$. Logo, $S = \emptyset$ e o resultado segue. □

Como consequência direta do resultado anterior, temos o seguinte corolário:

Corolário 8. *Em um domínio de Dedekind todo ideal não-nulo contém um produto de um ou mais ideais primos.*

Como queremos ser capazes de fatorar ideais, é interessante definir e estudar a inversa de um ideal. Com isso, temos a seguinte definição:

Definição 66 (Ideal fracionário)**.** *Sejam D um domínio de integridade e K seu corpo quociente. Um subconjunto não-nulo A de K com as propriedades:*

- $a, b \in A \Rightarrow a + b \in A$.
- $a \in A$, $r \in D \Rightarrow ra \in A$.
- *Existe* $\gamma \in D$ *com* $\gamma \neq 0$ *tal que* $\gamma A \subset D$.

é chamado de um ideal fracionário de D.

Note que, se A é um ideal fracionário de D e $A \subset D$, então A é um ideal de D. Ainda, todo ideal de D é também um ideal fracionário de D. Da definição anterior, vemos que se A é um ideal fracionário de D então:

$$A = \frac{1}{\gamma} I$$

em que $\gamma \in D \setminus \{0\}$ e I é um ideal de D. Note ainda que essa representação não é única, pois se $\delta \in D \setminus \{0\}$, então δI é um ideal de D e:

$$A = \frac{1}{\gamma\delta} \delta I$$

Em particular, se D é um domínio Noetheriano, então cada ideal I de D é finitamente gerado. Então, existem $\alpha_1, ..., \alpha_k \in D$ tais que:

$$I = \langle \alpha_1, ..., \alpha_k \rangle$$

Assim:

$$A = \frac{1}{\gamma} I = \frac{1}{\gamma} \langle \alpha_1, ..., \alpha_k \rangle = \left\langle \frac{\alpha_1}{\gamma}, ..., \frac{\alpha_k}{\gamma} \right\rangle$$

ou seja, todo ideal fracionário A de D é também finitamente gerado. Por fim, note ainda que, se A e B são ideais fracionários de D e γ e δ pertencentes a $D \setminus \{0\}$ satisfazem:

$$A = \frac{1}{\gamma} I \text{ e } B = \frac{1}{\delta} J$$

com I e J ideais de D, então $\alpha = \gamma\delta \in D \setminus \{0\}$ é tal que:

$$A = \frac{1}{\alpha} I' \text{ e } B = \frac{1}{\alpha} J'$$

com $I' = \delta I$ e $J' = \gamma J$ ideais de D. Assim, podemos definir $A + B$ e AB como sendo:

$$A + B = \frac{1}{\alpha}(I' + J') \text{ e } AB = \frac{1}{\alpha^2} I'J'$$

donde vemos que $A + B$ e AB são ideais fracionário de D e que as propriedades mostradas para a adição e o produto de ideais são também válidas para a adição e o produto de ideais fracionários.

Definamos então o conjunto $\tilde{P}$ para um ideal primo P.

Definição 67. *Sejam D um domínio de integridade e K o corpo quociente de D. Para cada ideal primo P de D definamos o conjunto $\tilde{P}$ como:*

$$\tilde{P} = \{\alpha \in K \ \mid \ \alpha P \subset D\}$$

Teorema 93. *Sejam D um domínio de integridade e P um ideal primo de D. Então $\tilde{P}$ é um ideal fracionário de D.*

Demonstração.

- Se $a, b \in \tilde{P}$ então $aP \subset D$ e $bP \subset D$. Então $(a+b)P \subset aP + bP \subset D$, donde $a + b \in \tilde{P}$.
- Se $a \in \tilde{P}$ e $r \in D$, então como $aP \subset D$, temos $raP \subset aP \subset D$, donde $ra \in \tilde{P}$.
- Seja $\pi \in P \setminus \{0\}$. Para todo $a \in \tilde{P}$, temos $aP \subset D$, donde $a\pi \in D$. Assim, $\pi\tilde{P} \subset D$.

  Portanto, $\tilde{P}$ é um ideal fracionário de D. □

Mostraremos, no próximo resultado, que em um domínio de Dedekind, $\tilde{P}$ é o inverso do ideal primo P.

Teorema 94. *Sejam D um domínio de Dedekind e P um ideal primo de D. Então $P\tilde{P} = D = \langle 1 \rangle$.*

Demonstração. Primeiramente, mostraremos que:

$$P\tilde{P} = D \text{ ou } P\tilde{P} = P$$

Como $\tilde{P}$ e P são ambos ideais fracionários de D, segue pelas observações anteriores que $P\tilde{P}$ é um ideal fracionário de D. Mostremos que $P\tilde{P} \subset D$. De fato, se $x \in P\tilde{P}$, então existem $r_1, ..., r_n \in P$ e $s_1, ..., s_n \in \tilde{P}$ tais que:

$$x = r_1 s_1 + ... + r_n s_n$$

Dado $i \in \{1, ..., n\}$, como $s_i \in \tilde{P}$, segue, por definição, que $s_i P \subset D$. Em particular, $r_i s_i \in s_i P \subset D$. Logo, $x \in D$. Portanto, $P\tilde{P} \subset D$ e, pelas considerações anteriores, temos que $P\tilde{P}$ é um ideal de D. Como $1P = P \subset D$, segue que $1 \in \tilde{P}$, donde $P \subset P\tilde{P}$. Ainda,

como P é um ideal primo e D é um domínio de Dedekind, segue que P é um ideal maximal. Portanto, $P\tilde{P} = P$ ou $P\tilde{P} = D$.

Mostremos agora que $D \subset \tilde{P}$. Se $a \in D$ então $aP \subset P \subset D$, de forma que $a \in \tilde{P}$. Logo, $D \subset \tilde{P}$. Mostremos ainda que $D \subsetneq \tilde{P}$. Seja $\beta \in P \setminus \{0\}$. Pelo Teorema 8 existem ideais primos $P_1, ..., P_k$ de D tais que:

$$P_1...P_k \subset \langle \beta \rangle$$

Escolhamos k como sendo o menor inteiro positivo tal que a inclusão acima valha. Como:

$$P_1...P_k \subset \langle \beta \rangle \subset P$$

e P é um ideal primo, temos:

$$P_i \subset P$$

para algum $i \in \{1, ..., k\}$. Reordenando os índices se necessário, podemos supor que $P_1 \subset P$. Uma vez que D é um domínio de Dedekind, segue que P_1 é um ideal maximal, e então:

$$P_1 = P$$

Consideremos agora duas possibilidades:

- Caso $k = 1$: Neste caso, $P = P_1 = \langle \beta \rangle$. Como $\beta \neq 0$, podemos definir $\gamma = \dfrac{1}{\beta} \in K$. Suponha que $\gamma \in D$. Então $\beta \in U(D)$ e $P = \langle \beta \rangle = D$, contradizendo que P é um ideal primo. Logo, $\gamma \notin D$ e:

  $$\gamma P = \frac{1}{\beta} \langle \beta \rangle = \langle 1 \rangle = D$$

  donde $\gamma \in \tilde{P}$. Então, $\gamma \in \tilde{P} \setminus D$, donde $\tilde{P} \setminus D \neq \emptyset$.

- Caso $k \geq 2$: Neste caso, pela minimalidade de k, temos:

  $$P_2...P_k \not\subset \langle \beta \rangle$$

  Então existe $\delta \in P_2...P_k$ tal que $\delta \notin \langle \beta \rangle$. Como $\beta \neq 0$, podemos definir $\gamma = \dfrac{\delta}{\beta} \in K$. Como $\delta \notin \langle \beta \rangle$, vemos que $\gamma = \dfrac{\delta}{\beta} \notin D$. Entretanto:

  $$P \langle \delta \rangle = P_1 \langle \delta \rangle \subset P_1...P_k \subset \langle \beta \rangle$$

  donde:

  $$P\gamma = P\frac{\delta}{\beta} \subset D$$

  Logo $\gamma \in \tilde{P} \setminus D$. Assim, $\tilde{P} \setminus D \neq \emptyset$.

Com isso, mostramos que:

$$D \subsetneq \tilde{P}$$

Por fim, mostraremos que:

$$P\tilde{P} = D$$

Sabemos que $P\tilde{P} = P$ ou $P\tilde{P} = D$. Mostremos que $P\tilde{P} \neq P$. Suponha que $P\tilde{P} = P$. Sejam $a, b \in \tilde{P}$. Então $aP, bP \subset P\tilde{P} = P$. Assim:

$$abP \subset aP \subset P$$

donde $ab \in \tilde{P}$. Portanto, $\tilde{P}$ é fechado para o produto. Logo, $\tilde{P}$ é um domínio de integridade com $D \subsetneq \tilde{P} \subset K$. Como D é um domínio Noetheriano, todos seus ideais (e, consequentemente, todos os seus ideais fracionários) são finitamente gerados. Logo, $\tilde{P}$ é um ideal fracionário de D finitamente gerado. Em particular, $\tilde{P}$ é um D-módulo finitamente gerado. Pelo Teorema 48, $\tilde{P}$ é inteiro sobre D. Entretanto, D é inteiramente fechado, donde segue que $D = \tilde{P}$. Tal fato contradiz $D \subsetneq \tilde{P}$. Portanto, $P\tilde{P} = D$. □

6.3 FATORAÇÃO EM IDEAIS PRIMOS

Usaremos do último teorema da seção anterior para provar a propriedade que, em domínios de Dedekind, todo ideal próprio de D pode ser expresso unicamente como produto de ideais primos.

Teorema 95. *Se D é um domínio de Dedekind e I é um ideal de D com $I \neq \langle 0 \rangle, \langle 1 \rangle$, então I é um produto de ideais primos. Se existem $P_1, ..., P_k, Q_1, ..., Q_r$ ideais primos de D tais que:*

$$I = P_1P_2...P_k = Q_1Q_2...Q_r$$

então $k = r$ e, após reordenarmos índices (se necessário), temos:

$$P_i = Q_i \text{ para todo } i \in \{1, ..., k\}$$

Demonstração. Suponha que exista um ideal I de D, com $I \neq \langle 0 \rangle, \langle 1 \rangle$, tal que I não é o produto de ideais primos. Como D é um domínio de Dedekind, D é Noetheriano, e pela condição maximal (a qual D satisfaz pelo Teorema 36), existe um ideal A de D maximal com respeito a propriedade de não ser o produto de ideais primos. Pelo Teorema 92, existem ideais primos $P_1, ..., P_k$ de D tais que:

$$P_1...P_k \subset A$$

Seja k o menor inteiro positivo com esta propriedade. Se $k = 1$, então $P_1 \subset A \subset D$. Como P_1 é um ideal primo de D, P_1 é um ideal maximal de D, pois D é um domínio de

Dedekind. Logo, $A = P_1$, o que contradiz A não ser o produto de ideais primos. Então $k \geq 2$. Pelo Teorema 94, temos $\tilde{P}_1 P_1 = D$, donde:

$$\tilde{P}_1 P_1 P_2 ... P_k = D P_2 ... P_k = P_2 ... P_k$$

Então:

$$P_2 ... P_k \subset \tilde{P}_1 A$$

Pela demonstração do Teorema 94 temos que $D \subset \tilde{P}_1$, donde $A \subset \tilde{P}_1 A$. Se $A = \tilde{P}_1 A$, então:

$$P_2 ... P_k \subset A$$

o que contradiz a minimalidade de k. Então $A \subsetneq \tilde{P}_1 A$. Como $\tilde{P}_1 A$ é um ideal de D, pela maximalidade de A, temos:

$$\tilde{P}_1 A = Q_2 ... Q_h$$

para ideais primos $Q_2, ..., Q_h$. Então:

$$A = AD = A\tilde{P}_1 P_1 = P_1 Q_2 ... Q_h$$

é também um produto de ideais primos, o que contradiz A não ser o produto de ideais primos. Logo, todo ideal $I \neq \langle 0 \rangle, \langle 1 \rangle$ de D é um produto de ideais primos.

Suponha que exista um ideal $I \neq \langle 0 \rangle, \langle 1 \rangle$ de D tal que a fatoração como produto de ideais primos de D não é única. Pela condição maximal, podemos tomar um ideal B maximal com relação a esta propriedade. Então, existem duas fatorações distintas de B, isto é, existem $P_1, ..., P_k, Q_1, ..., Q_r$ ideais primos de D tais que:

$$B = P_1 ... P_k = Q_1 ... Q_r$$

Como $P_1 ... P_k \subset Q_1$ e Q_1 é um ideal primo, segue pelo Teorema 15 que existe $i \in \{1, ..., k\}$ tal que:

$$P_i \subset Q_1$$

Reordenando os índices se necessário, podemos supor que $P_1 \subset Q_1$. Como P_1 é um ideal primo de D (domínio de Dedekind), segue que P_1 é um ideal maximal. Então:

$$P_1 = Q_1$$

Assim:

$$B\tilde{P}_1 = \tilde{P}_1 P_1 P_2 ... P_k = P_2 ... P_k$$

e:

$$B\tilde{P}_1 = B\tilde{Q}_1 = \tilde{Q}_1 Q_1 ... Q_r = Q_2 ... Q_r$$

Se $B\tilde{P}_1 = B$, então $B\tilde{P}_1 P_1 = BP_1$, donde $B = BP_1$. Definamos o ideal fracionário $\tilde{B}$ de D como sendo:

$$\tilde{B} = \tilde{P}_1 ... \tilde{P}_k$$

Então:

$$B\tilde{B} = P_1...P_k\tilde{P}_1...\tilde{P}_k = P_1\tilde{P}_1...P_k\tilde{P}_k = D$$

donde:

$$D = B\tilde{B} = B\tilde{P}_1\tilde{B} = P_1$$

o que contradiz P_1 ser um ideal primo (e, consequentemente, próprio) de D. Então $B\tilde{P}_1 \neq B$. Como $D \subset \tilde{P}_1$, temos $B \subset B\tilde{P}_1$. Assim, devemos ter:

$$B \subsetneq B\tilde{P}_1$$

Como $B\tilde{P}_1$ é um ideal de D que contém B estritamente, pela maximalidade de B segue que $B\tilde{P}_1$ tem exatamente uma fatoração como o produto de ideais primos. Então, de $B\tilde{P}_1 = P_2...P_k = Q_2...Q_r$, deduzimos que $k-1 = r-1$ (donde $k = r$) e, após reordenarmos os índices, se necessário, obtemos $P_i = Q_i$ para $i \in \{2, ..., k\}$. Isso implica que ambas as fatorações de B são iguais, o que é um absurdo. Com isso, o resultado segue. □

Como um caso particular do teorema anterior, temos o seguinte resultado:

Corolário 9. *Seja K um corpo de números algébricos. Então todo ideal próprio de O_K pode ser expresso unicamente como o produto de ideais primos de O_K.*

Demonstração. Esse resultado segue como consequência direta dos Teoremas 90 e 95. □

Seja A um ideal próprio de um domínio de Dedekind D. Pelo Teorema 95, sabemos que A pode ser escrito unicamente (a menos de ordem) na forma:

$$A = Q_1...Q_r$$

com $Q_1, ..., Q_r$ ideais primos de D. Sejam $P_1, ..., P_n$ os diferentes ideais primos dentre os ideais $Q_1, ..., Q_r$. Suponha que cada P_i ocorre a_i vezes dentre $Q_1, ..., Q_r$ de tal forma que $a_i \geq 1$ e $a_1 + ... + a_n = r$. Então:

$$A = P_1^{a_1}...P_n^{a_n}$$

sendo $a_1, ..., a_n$ inteiros positivos. Pelo Teorema 95, essa representação é única (a menos de ordem). Definamos também que $D = P_1^0P_2^0...P_n^0$, de forma que D é produto de 0 ideais primos. Com estas convenções, temos que todo ideal não-nulo de um domínio de Dedekind pode ser escrito de maneira única (a menos de ordem) como um produto de potências de ideais primos.

Sejam A e B ideais não-nulos de um domínio de Dedekind D. Então AB é um ideal não-nulo de D. Sejam $P_1, ..., P_n$ ideais primos distintos de D tais que cada um deles ocorre na fatoração de pelo menos um dos ideais A, B ou AB. Então:

$$A = \prod_{i=1}^{n} P_i^{a_i}, B = \prod_{i=1}^{n} P_i^{b_i}, \text{ e } AB = \prod_{i=1}^{n} P_i^{c_i}$$

com a_i, b_i, c_i inteiros não-negativos para $i \in \{1, ..., n\}$. Assim:

$$\prod_{i=1}^{n} P_i^{c_i} = AB = \prod_{i=1}^{n} P_i^{a_i} \prod_{i=1}^{n} P_i^{b_i} = \prod_{i=1}^{n} P_i^{a_i+b_i}$$

Pelo Teorema 95, segue que:

$$c_i = a_i + b_i \text{ para todo } i \in \{1, ..., n\}$$

Definição 68 (Divisibilidade de ideais)**.** *Sejam D um domínio de Dedekind e A e B ideais não-nulos de D. Dizemos que A divide B, e escrevemos $A \mid B$, se existe um ideal C de D tal que $B = AC$.*

Se $A = \prod_{i=1}^{n} P_i^{a_i}$, $B = \prod_{i=1}^{n} P_i^{b_i}$, com $P_1, ..., P_n$ ideais primos distintos de D e $a_1, ..., a_n, b_1, ..., b_n$ inteiros não-negativos, então:

$$A \mid B \Leftrightarrow a_i \leq b_i \text{ para } i \in \{1, ..., n\}$$

Estenderemos agora a representação de ideais como produto de ideais primos para ideais fracionários.

Seja A um ideal fracionário não-nulo de um domínio de Dedekind D. Sejam $a, b \in D \setminus \{0\}$ dois denominadores comuns de A (isto é, $aA \subset D$ e $bA \subset D$). Então:

$$\langle a \rangle A = B \text{ e } \langle b \rangle A = C$$

com B e C ideais não-nulos de D. Suponha que:

$$\langle a \rangle = \prod_{i=1}^{n} P_i^{r_i}, B = \prod_{i=1}^{n} P_i^{s_i}$$
$$\langle b \rangle = \prod_{i=1}^{n} P_i^{t_i}, C = \prod_{i=1}^{n} P_i^{u_i}$$

em que $P_1, ..., P_n$ são ideais primos distintos de D e r_i, s_i, t_i, u_i são inteiros não-negativos para $i \in \{1, ..., n\}$. Então, como:

$$\langle a \rangle C = \langle a \rangle (\langle b \rangle A) = \langle b \rangle (\langle a \rangle A) = \langle b \rangle B$$

temos:

$$\prod_{i=1}^{n} P_i^{r_i+u_i} = \prod_{i=1}^{n} P_i^{s_i+t_i}$$

de forma que, pelo Teorema 95, segue que:

$$r_i + u_i = s_i + t_i, \text{ para } i \in \{1, ..., n\}$$

Portanto, podemos definir a fatoração em ideais primos do ideal fracionário A como sendo:

$$A = \prod_{i=1}^{n} P_i^{s_i - r_i}$$

e esta definição é válida pois independe da escolha do denominador comum de A. Com esta notação, como $P\tilde{P} = \langle 1 \rangle$ para todo ideal primo P de D, temos:

$$\tilde{P} = P^{-1}$$

Se $P_1, ..., P_n$ são ideais primos tais que:

$$\prod_{i=1}^{n} P_i^{a_i} = \prod_{i=1}^{n} P_i^{b_i}$$

em que a_i, b_i são inteiros para todo $i \in \{1, ..., n\}$, então multiplicando ambos os termos da equação por $\prod_{i=1}^{n} P_i^M$, em que M é um inteiro positivo tal que $a_i + M > 0$ e $b_i + M > 0$ para todo $i \in \{1, ..., n\}$ (por exemplo, $M = \max\{|a_1|, ..., |a_n|, |b_1|, ..., |b_n|\} + 1 \in \mathbb{N}$), e usando do Teorema 95, obtemos que $a_i + M = b_i + M$ para todo $i \in \{1, ..., n\}$, donde $a_i = b_i$ para todo $i \in \{1, ..., n\}$. Portanto, a representação de um ideal fracionário não-nulo de D como um produto de ideais primos de D é única.

Pelas considerações anteriores, segue o seguinte resultado:

Teorema 96. *O conjunto de todos os ideais fracionários de um domínio de Dedekind D forma um grupo abeliano com respeito a multiplicação. A identidade do grupo é $\langle 1 \rangle = D$ e a inversa de $A = \prod_{i=1}^{n} P_i^{a_i}$, com $P_1, ..., P_n$ ideais primos distintos de D e $a_1, ..., a_n \in \mathbb{Z}$, é:*

$$A^{-1} = \prod_{i=1}^{n} P_i^{-a_i}$$

Como consequência do teorema anterior, temos o seguinte resultado:

Corolário 10. *Sejam K um corpo de números algébricos e O_K seu anel de inteiros. Então o conjunto de todos os ideais fracionários não-nulos de O_K forma um grupo abeliano $I(K)$ com respeito a multiplicação.*

Demonstração. Esse resultado é consequência direta dos Teoremas 90 e 96. □

6.4 ORDEM DE UM IDEAL COM RESPEITO A UM IDEAL PRIMO

Seja A um ideal fracionário não-nulo de um domínio de Dedekind D. Então, A pode ser escrito unicamente na forma:

$$A = \prod_{i=1}^{n} P_i^{a_i}$$

em que cada P_i é um ideal primo distinto de D e $a_i \in \mathbb{Z}$. Com esta notação, podemos definir a ordem de um ideal com respeito a um ideal primo.

Definição 69 (Ordem de um ideal com respeito a um ideal primo)**.** *A ordem de A com respeito ao ideal primo P_i (com $i \in \{1, ..., n\}$), denotada por* $\text{ord}_{P_i}(A) = a_i$*. Se P é um ideal primo de D e $P \notin \{P_1, ..., P_n\}$, definimos:*

$$\text{ord}_P(A) = 0$$

Em particular, temos pela definição anterior que $\text{ord}_P(\langle 1 \rangle) = 0$ e $\text{ord}_P(P^k) = k$ para todo ideal primo P de D.

Podemos então estender o conceito de divisibilidade de ideais para ideais fracionários.

Definição 70 (Divisibilidade de ideais fracionários)**.** *Sejam D um domínio de Dedekind e A e B ideais fracionários não-nulos de D. Dizemos que A divide B, e escrevemos $A \mid B$, se existe um ideal C de D tal que $B = AC$.*

Pela definição anterior e pelas considerações da seção anterior, temos que:

$$A \mid B \Leftrightarrow \text{ord}_P(A) \leq \text{ord}_P(B) \text{ para todos os ideais primos } P \text{ de } D$$

O próximo teorema nos dá uma condição necessária e suficiente para um ideal fracionário A dividir um ideal fracionário B.

Teorema 97. *Sejam D um domínio de Dedekind e A e B ideais fracionários não-nulos de D. Então:*

$$A \mid B \Leftrightarrow B \subset A$$

Demonstração. Como A é um ideal fracionário não-nulo de D, A^{-1} é um ideal fracionário não-nulo de D. Então BA^{-1} é um ideal fracionário não-nulo de D. Então:

$$\begin{aligned} B \subset A &\Leftrightarrow BA^{-1} \subset AA^{-1} \Leftrightarrow \\ &\Leftrightarrow BA^{-1} \subset D \Leftrightarrow \\ &\Leftrightarrow BA^{-1} \text{ é um ideal de } D \Leftrightarrow \\ &\Leftrightarrow BA^{-1} = C \text{ para algum ideal } C \text{ de } D \Leftrightarrow \\ &\Leftrightarrow B = AC \text{ para algum ideal } C \text{ de } D \Leftrightarrow \\ &\Leftrightarrow A \mid B \end{aligned}$$

□

Provaremos agora algumas propriedades da função $\text{ord}_P(A)$.

Teorema 98. *Sejam D um domínio de Dedekind, P um ideal primo de D e A e B ideais fracionários não-nulos de D. Então:*

1. $\mathrm{ord}_P(AB) = \mathrm{ord}_P(A) + \mathrm{ord}_P(B)$.

2. $\mathrm{ord}_P(A+B) = \min\{\mathrm{ord}_P(A), \mathrm{ord}_P(B)\}$.

Demonstração. 1. Pela definição da ordem de um ideal com respeito a um ideal primo, temos:

$$A = \prod_P P^{\mathrm{ord}_P(A)} \text{ e } B = \prod_P P^{\mathrm{ord}_P(B)}$$

em que os produtos são tomados sobre todos os ideais primos P de D, donde:

$$\prod_P P^{\mathrm{ord}_P(AB)} = AB = \prod_P P^{\mathrm{ord}_P(A)+\mathrm{ord}_P(B)}$$

Pela unicidade da fatoração como produto de ideais primos, temos:

$$\mathrm{ord}_P(AB) = \mathrm{ord}_P(A) + \mathrm{ord}_P(B)$$

para todos os ideais primos P de D.

2. Seja $C = A + B$. Como A e B são ideais fracionários não-nulos, C também é um ideal fracionário não-nulo. Então:

$$AC^{-1} + BC^{-1} = (A+B)C^{-1} = CC^{-1} = D$$

Com isso, $AC^{-1} \subset AC^{-1} + BC^{-1} = D$ e $BC^{-1} \subset AC^{-1} + BC^{-1} = D$. Logo, AC^{-1} e BC^{-1} são ambos ideais de D. Suponha que $AC^{-1} \subset P$ e $BC^{-1} \subset P$. Neste caso:

$$D = AC^{-1} + BC^{-1} \subset P + P = P$$

o que é impossível. Logo, $AC^{-1} \not\subset P$ ou $BC^{-1} \not\subset P$. Pelo Teorema 97, isso implica em $P \nmid AC^{-1}$ ou $P \nmid BC^{-1}$, donde:

$$\min\{\mathrm{ord}_P(AC^{-1}), \mathrm{ord}_P(BC^{-1})\} = 0$$

Por fim, pelo item anterior, obtemos:

$$\min\{\mathrm{ord}_P(A), \mathrm{ord}_P(B)\} = \mathrm{ord}_P(C) = \mathrm{ord}_P(A+B)$$

□

Definamos agora a ordem de um elemento não-nulo com respeito a um ideal primo.

Definição 71 (Ordem de um elemento não-nulo com respeito a um ideal primo)**.** *Seja D um domínio de Dedekind com corpo quociente K. Para $\alpha \in K \setminus \{0\}$, definimos:*

$$\mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\langle\alpha\rangle)$$

para todo ideal primo P de D.

O próximo resultado nos permite identificar quando um elemento α pertence a um ideal A de D baseado nas ordens de α e de A com respeito a ideais primos P.

Teorema 99. *Sejam D um domínio de Dedekind, K seu corpo quociente, A um ideal não-nulo de D e $\alpha \in K \setminus \{0\}$. Então:*

$$\alpha \in A \Leftrightarrow \mathrm{ord}_P(\alpha) \geq \mathrm{ord}_P(A) \text{ para todo ideal primo } P \text{ de } D$$

Demonstração. Temos:

$$\begin{aligned}\alpha \in A &\Leftrightarrow \langle\alpha\rangle \subset A \Leftrightarrow \\ &\Leftrightarrow A \mid \langle\alpha\rangle \text{ (pelo Teorema 97)} \Leftrightarrow \\ &\Leftrightarrow \mathrm{ord}_P(A) \leq \mathrm{ord}_P(\langle\alpha\rangle) = \mathrm{ord}_P(\alpha) \text{ para todo ideal primo } P \text{ de } D\end{aligned}$$

□

Assim como mostramos propriedades básicas da ordem de um ideal com respeito a um ideal primo, mostraremos agora propriedades básicas da ordem de um elemento com respeito a um ideal primo.

Teorema 100. *Sejam D um domínio de Dedekind com corpo quociente K e P um ideal primo de D.*

1. *Para $\alpha, \beta \in K^* = K \setminus \{0\}$:*

$$\mathrm{ord}_P(\alpha\beta) = \mathrm{ord}_P(\alpha) + \mathrm{ord}_P(\beta)$$

2. *Para $\alpha, \beta \in K^*$ com $\alpha + \beta \in K^*$:*

$$\mathrm{ord}_P(\alpha + \beta) \geq \min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}$$

3. *Se $\alpha, \beta, \alpha + \beta \in K^*$ e $\mathrm{ord}_P(\alpha) \neq \mathrm{ord}_P(\beta)$, então:*

$$\mathrm{ord}_P(\alpha + \beta) = \min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}$$

Demonstração. 1. Se P é um ideal primo de D, então:

$$\begin{aligned}\mathrm{ord}_P(\alpha\beta) &= \mathrm{ord}_P(\langle\alpha\beta\rangle) = \\ &= \mathrm{ord}_P(\langle\alpha\rangle\langle\beta\rangle) = \\ &= \mathrm{ord}_P(\langle\alpha\rangle) + \mathrm{ord}_P(\langle\beta\rangle) = \\ &= \mathrm{ord}_P(\alpha) + \mathrm{ord}_P(\beta)\end{aligned}$$

2. Como $\alpha + \beta \in \langle\alpha\rangle + \langle\beta\rangle$, temos pelo item 2 do Teorema 98 e pelo Teorema 99 que:

$$\begin{aligned}\mathrm{ord}_P(\alpha+\beta) &\geq \mathrm{ord}_P(\langle\alpha\rangle + \langle\beta\rangle) = \\ &= \min\{\mathrm{ord}_P(\langle\alpha\rangle), \mathrm{ord}_P(\langle\beta\rangle)\} = \\ &= \min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}\end{aligned}$$

3. Sem perda de generalidade, podemos supor que:

$$\mathrm{ord}_P(\alpha) > \mathrm{ord}_P(\beta)$$

Então, pelo item 2, temos:

$$\mathrm{ord}_P(\alpha+\beta) \geq \mathrm{ord}_P(\beta)$$

Assim:

$$\begin{aligned}\mathrm{ord}_P(\beta) &= \mathrm{ord}_P((\alpha+\beta)-\alpha) \geq \\ &\geq \min\{\mathrm{ord}_P(\alpha+\beta), \mathrm{ord}_P(\alpha)\} = \\ &= \mathrm{ord}_P(\alpha+\beta) \geq \\ &\geq \mathrm{ord}_P(\beta)\end{aligned}$$

Portanto:

$$\mathrm{ord}_P(\alpha+\beta) = \mathrm{ord}_P(\beta) = \min\{\mathrm{ord}_P(\alpha), \mathrm{ord}_P(\beta)\}$$

□

O próximo teorema nos mostra que sempre podemos encontrar um elemento do corpo quociente de um domínio de Dedekind que satisfaça uma determinada condição sobre os valores de suas ordens com respeito a ideais primos.

Teorema 101. *Sejam D um domínio de Dedekind e K o seu corpo quociente. Dados um conjunto finito de ideais primos distintos $\{P_1, ..., P_k\}$ de D e um conjunto de inteiros $\{a_1, ..., a_k\}$, existe $\alpha \in K$ tal que:*

$$\mathrm{ord}_{P_i}(\alpha) = a_i \text{ para } i \in \{1, ..., k\}$$

e

$$\mathrm{ord}_P(\alpha) \geq 0 \text{ para } P \notin \{P_1, ..., P_k\}$$

Demonstração. Como:

$$P_1^{a_1} \prod_{i=2}^{k} P_i^{a_1+1} \mid P_1^{a_i+1} \prod_{i=2}^{k} P_i^{a_i+1}$$

pelo Teorema 97 temos:

$$P_1^{a_1+1} \prod_{i=2}^{k} P_i^{a_i+1} \subset P_1^{a_1} \prod_{i=2}^{k} P_i^{a_i+1}$$

Pela unicidade da fatoração, temos:

$$P_1^{a_1+1}\prod_{i=2}^{k}P_i^{a_i+1} \neq P_1^{a_1}\prod_{i=2}^{k}P_i^{a_i+1}$$

donde:

$$P_1^{a_1+1}\prod_{i=2}^{k}P_i^{a_i+1} \subsetneq P_1^{a_1}\prod_{i=2}^{k}P_i^{a_i+1}$$

Portanto, existe $\alpha_1 \in K$ tal que:

$$\alpha_1 \in P_1^{a_1}\prod_{i=2}^{k}P_i^{a_i+1} \text{ e } \alpha_1 \notin P_1^{a_1+1}\prod_{i=2}^{k}P_i^{a_i+1}$$

Então:

$$\text{ord}_{P_1}(\alpha_1) = a_1$$

e

$$\text{ord}_{P_i}(\alpha_1) \geq a_i + 1 \text{ para } i \neq 1$$

De maneira análoga, podemos definir $\alpha_j \in K$ para $j \in \{2, ..., k\}$ tais que:

$$\text{ord}_{P_j}(\alpha_j) = a_j$$

e

$$\text{ord}_{P_i}(\alpha_j) \geq a_i + 1 \text{ para } i \neq j$$

Definamos então $\alpha \in K$ como sendo:

$$\alpha = \alpha_1 + \alpha_2 + ... + \alpha_k$$

Então, pelo item 2 do Teorema 100, temos:

$$\text{ord}_{P_1}(\alpha_2 + ... + \alpha_k) \geq \min\{\text{ord}_{P_1}(\alpha_2), ..., \text{ord}_{P_1}(\alpha_k)\} \geq a_1 + 1 > \text{ord}_{P_1}(\alpha_1)$$

donde:

$$\begin{aligned}\text{ord}_{P_1}(\alpha) &= \min\{\text{ord}_{P_1}(\alpha_1), ..., \text{ord}_{P_1}(\alpha_k)\} = \min\{\text{ord}_{P_1}(\alpha_1), \text{ord}_{P_1}(\alpha_2 + ... + \alpha_k)\} = \\ &= \text{ord}_{P_1}(\alpha_1) = a_1\end{aligned}$$

Analogamente:

$$\text{ord}_{P_j}(\alpha) = a_j \text{ para } j \in \{2, ..., k\}$$

Por fim, para $P \neq P_1, ..., P_k$, temos:

$$\text{ord}_P(\alpha_i) \geq 0 \text{ para } i \in \{1, ..., k\}$$

de forma que:

$$\text{ord}_P(\alpha) \geq 0$$

□

Se D é um domínio de Dedekind com corpo quociente K, A é um ideal fracionário não-nulo de D e $a, b, c \in A$, escreveremos que:

$$a \equiv b \pmod{A} \text{ se, e somente se, } A \mid \langle a - b \rangle$$

Note que:

$$A \mid \langle a - b \rangle \Leftrightarrow \langle a - b \rangle \subset A \Leftrightarrow a - b \in A \Leftrightarrow a + A = b + A$$

Com estas observações e usando as propriedades dos ideais, segue que:

$$\begin{aligned}
&a \equiv a \pmod{A} \\
&a \equiv b \pmod{A} \Rightarrow b \equiv a \pmod{A} \\
&a \equiv b \pmod{A}, b \equiv c \pmod{A} \Rightarrow a \equiv c \pmod{A} \\
&a \equiv b \pmod{A} \Rightarrow ac \equiv bc \pmod{A}
\end{aligned}$$

Usando desta notação, enunciaremos e provaremos o Teorema chinês dos restos para ideais.

Teorema 102 (Teorema chinês dos restos)**.** *Sejam D um domínio de Dedekind e $\alpha_1, ..., \alpha_k \in D$.*

1. *Se $P_1, ..., P_k$ são ideais primos distintos de D e $a_1, ..., a_k$ são inteiros positivos, então existe $\alpha \in D$ tal que:*

$$\alpha \equiv \alpha_i \pmod{P_i^{a_i}} \text{ para } i \in \{1, ..., k\}$$

2. *Se $I_1, ..., I_k$ são ideais de D primos entre si dois a dois, então existe $\alpha \in D$ tal que:*

$$\alpha \equiv \alpha_i \pmod{I_i} \text{ para } i \in \{1, ..., k\}$$

Demonstração. 1. Considere o ideal de D:

$$Q_1 = P_1^{a_1} + P_2^{a_2} ... P_k^{a_k}$$

Suponha que P é um ideal primo tal que $P \mid Q_1$. Então, como:

$$P_1^{a_1} \subset Q_1, P_2^{a_2} ... P_k^{a_k} \subset Q_1$$

segue pelo Teorema 97 que:

$$Q_1 \mid P_1^{a_1}, Q_1 \mid P_2^{a_2} ... P_k^{a_k}$$

Portanto:

$$P \mid P_1^{a_1}, P \mid P_2^{a_2} ... P_k^{a_k}$$

Pela primeira das relações acima deduzimos que $P \mid P_1$, donde $P = P_1$. Então:

$$P_1 = P \mid P_2^{a_2}...P_k^{a_k}$$

o que contradiz P_1 ser um ideal primo distinto de $P_2, ..., P_k$. Então, não existe ideal primo dividindo Q_1. Portanto, $Q_1 = D$, donde $\langle 1 \rangle = P_1^{a_1} + P_2^{a_2}...P_k^{a_k}$. Assim, existem $x_1 \in P_1^{a_1}$ e $y_1 \in P_2^{a_2}...P_k^{a_k}$ tais que $x_1 + y_1 = 1$. Então:

$$y_1 \equiv 1 \pmod{P_1^{a_1}}, y_1 \equiv 0 \pmod{P_i^{a_i}} \text{ para } i \in \{2, ..., k\}$$

Analogamente, para $j \in \{2, ..., k\}$, podemos encontrar y_j tal que:

$$y_j \equiv 1 \pmod{P_j^{a_j}}, y_j \equiv 0 \pmod{P_i^{a_i}} \text{ para } i \neq j$$

Definamos então:

$$\alpha = \alpha_1 y_1 + ... + \alpha_k y_k \in D$$

Então, como $\alpha_2 y_2 + ... + \alpha_k y_k \in P_1^{a_1}$, temos:

$$\alpha \equiv \alpha_1 y_1 \equiv \alpha_1 \pmod{P_1^{a_1}}$$

Analogamente, $\alpha \equiv \alpha_j \pmod{P_j^{a_j}}$ para $j \in \{2, ..., k\}$

2. Dado $i \in \{1, ..., k\}$, sejam $P_{i,1}, ..., P_{i,k_i}$ ideais primos distintos de D tais que $I_i = \prod_{s=1}^{k_i} P_{i,s}^{a_{i,s}}$, com $a_{i,s}$ inteiro positivo para todo $s \in \{1, ..., k_i\}$. Dado $j \in \{1, ..., k\} \setminus \{i\}$, como I_i e I_j são primos entre si, temos que $P_{i,s}$ e $P_{j,r}$ são ideais primos distintos de D para todos $s \in \{1, ..., k_i\}$ e $r \in \{1, ..., k_j\}$. Segue então que o sistema:

$$\alpha \equiv \alpha_i \pmod{I_i} \text{ para } i \in \{1, ..., k\}$$

é equivalente ao sistema:

$$\alpha \equiv \alpha_i \pmod{P_{i,s}^{a_{i,s}}} \text{ para todos } i \in \{1, ..., k\}, s \in \{1, ..., k_i\}$$

Pelo item 1, sabemos que existe $\alpha \in D$ que satisfaz o sistema acima. Portanto, existe $\alpha \in D$ tal que:

$$\alpha \equiv \alpha_i \pmod{I_i} \text{ para } i \in \{1, ..., k\}$$

□

6.5 GERADORES DE IDEAIS EM UM DOMÍNIO DE DEDEKIND

Por fim, mostraremos que todo ideal fracionário de um domínio de Dedekind é gerado por, no máximo, dois elementos.

Teorema 103. *Sejam D um domínio de Dedekind e A um ideal fracionário de D. Então A é gerado por, no máximo, dois elementos.*

Demonstração. Se $A = \{0\}$, então $A = \langle 0 \rangle$ e se $A = D$, então $A = \langle 1 \rangle$. Podemos então supor que $A \neq \langle 0 \rangle, \langle 1 \rangle$. Seja $\beta \in A$, com $\beta \neq 0$ e $\beta \notin U(D)$. Então $\langle \beta \rangle \subset A$, donde $A \mid \langle \beta \rangle$. Portanto, existe um ideal B de D não-nulo tal que:

$$\langle \beta \rangle = AB$$

Sejam $P_1, ..., P_n$ o conjunto de ideais primos distintos para os quais:

$$\text{ord}_{P_i}(A) \neq 0 \text{ ou } \text{ord}_{P_i}(AB) \neq 0$$

Este conjunto é não-vazio pois $A \neq D$. Pelo Teorema 101 existe $\alpha \in K$ (o corpo quociente de D) tal que:

$$\begin{aligned} \text{ord}_{P_i}(\alpha) &= \text{ord}_{P_i}(A) \text{ para } i \in \{1, ..., n\} \\ \text{ord}_P(\alpha) &\geq 0, \text{ para } P \neq P_1, ..., P_n \end{aligned}$$

Para $P \neq P_1, ..., P_n$, temos $\text{ord}_P(A) = 0$ donde:

$$\text{ord}_P(\alpha) \geq \text{ord}_P(A) \text{ para todos os ideais primos } P$$

Então, $\alpha \in A$. Para $i = 1, 2, ..., n$, temos:

$$\begin{aligned} \text{ord}_{P_i}(A) &= \min\{\text{ord}_{P_i}(A), \text{ord}_{P_i}(AB)\} (\text{pois } B \text{ é um ideal de } D) = \\ &= \min\{\text{ord}_{P_i}(\alpha), \text{ord}_{P_i}(AB)\} = \\ &= \min\{\text{ord}_{P_i}(\langle \alpha \rangle), \text{ord}_{P_i}(AB)\} = \\ &= \text{ord}_{P_i}(\langle \alpha \rangle + AB) \end{aligned}$$

pelo item 2 do Teorema 98. Para $P \neq P_1, ..., P_n$, temos $\text{ord}_P(A) = \text{ord}_P(AB) = 0$, de forma que:

$$\begin{aligned} \text{ord}_P(A) &= \min\{\text{ord}_P(\alpha), \text{ord}_P(AB)\} = \\ &= \min\{\text{ord}_P(\langle \alpha \rangle), \text{ord}_P(AB)\} = \\ &= \text{ord}_P(\langle \alpha \rangle + AB) \end{aligned}$$

pelo item 2 do Teorema 98. Portanto:

$$\text{ord}_P(A) = \text{ord}_P(\langle \alpha \rangle + AB) \text{ para todos os ideais primos } P \text{ de } D$$

Logo:

$$A = \langle \alpha \rangle + AB$$

Com isso, temos:

$$A = \langle \alpha \rangle + \langle \beta \rangle = \langle \alpha, \beta \rangle$$

□

7 EQUAÇÕES DIOFANTINAS

Estudaremos agora equações diofantinas não-lineares utilizando a teoria construída ao longo do texto. Em particular, veremos a utilidade da fatoração em ideais e como podemos usar a fatoração única para encontrar as soluções de equações diofantinas. Para isso, antes iremos definir mais alguns conceitos:

7.1 NORMA DE UM IDEAL FRACIONÁRIO, UNIDADES FUNDAMENTAIS E GRUPOS DE CLASSE

Nesta seção, definiremos o grupo de classe de um corpo de números algébricos e o número de classe do corpo, além da norma de um ideal fracionário e o conceito de unidade fundamental. Além disso, enunciaremos alguns resultados importantes sobre estes conceitos, cujas demonstrações serão omitidas por fugirem do escopo deste texto.

Vimos que os ideais fracionários não-nulos do anel de inteiros O_K de um corpo de números algébricos formam um grupo multiplicativo $I(K)$, conforme o Corolário 10. Os ideais principais em $I(K)$ são da forma $\langle\alpha\rangle = \{r\alpha \mid r \in O_K\}$ para algum $\alpha \in K^*$ e eles formam um subgrupo $P(K)$ de $I(K)$, uma vez que:

$$\langle\alpha\rangle \langle\beta\rangle^{-1} = \left\langle\alpha\beta^{-1}\right\rangle \in P(K)$$

para $\alpha, \beta \in K^*$. Como o grupo $I(K)$ é abeliano, segue que $P(K)$ é um subgrupo normal de $I(K)$ e, portanto, o grupo quociente $\dfrac{I(K)}{P(K)}$ está bem definido e é abeliano.

Definição 72 (Grupo de classe)**.** *Sejam K um corpo de números algébricos, $I(K)$ o grupo de ideais fracionários não-nulos de O_K e $P(K)$ o subgrupo de ideais principais de $I(K)$. Então o grupo quociente $\dfrac{I(K)}{P(K)}$ é chamado de grupo de classe de K e é denotado por $H(K)$.*

Denotaremos o elemento de $H(K)$ contendo um ideal fracionário A não-nulo como $[A]$, e o chamaremos de classe de ideais de A. Se A e B pertencerem à mesma classe de ideais, diremos que A é equivalente a B e escreveremos $A \sim B$. Note que:

$$\begin{aligned} A \sim B &\Leftrightarrow AP(K) = BP(K) \Leftrightarrow \\ &\Leftrightarrow A^{-1}B \in P(K) \Leftrightarrow \\ &\Leftrightarrow A^{-1}B = \langle\alpha\rangle \text{ para algum } \alpha \in K^* \Leftrightarrow \\ &\Leftrightarrow B = A\langle\alpha\rangle \text{ para algum } \alpha \in K^* \Leftrightarrow \\ &\Leftrightarrow \langle a\rangle A = \langle b\rangle B \text{ para algum par } a, b \in O_K \setminus \{0\} \end{aligned}$$

Um importante resultado provado por Minkowski, cuja demonstração omitiremos, é o de que $H(K)$ é sempre um grupo finito. Essa demonstração pode ser encontrada em (1). Tal fato nos leva a seguinte definição:

Definição 73 (Número de classe)**.** *Seja K um corpo de números algébricos. A ordem do grupo de classe $H(K)$ é chamada de número de classe de K e é denotada por $h(K)$.*

Note que a unidade em $H(K)$ é $[\langle 1\rangle]$ (a qual é também a classe de qualquer ideal principal) e que, se A e B são ideais fracionários não-nulos de O_K, $[AB] = [A][B]$ e $[A^{-1}] = [A]^{-1}$. Note ainda que $[A] \in H(K)$, donde, por um resultado conhecido da teoria dos grupos (que pode ser encontrado em (3)), segue que $[A]^{\operatorname{ord} H(K)} = [A]^{h(K)} = [1]$.

Provaremos agora um resultado, que será usado em alguns teoremas mais a frente.

Teorema 104. *Sejam K um corpo de números algébricos, h o número de classe de K e A um ideal de O_K tal que A^k é um ideal principal para algum k inteiro positivo coprimo com h. Então A é um ideal principal.*

Demonstração. Seja $[A]$ a classe de ideais de A. Pelas observações anteriores, temos que $[A^h] = [A]^h = [\langle 1\rangle] = I$, donde $A^h \in P(K)$, ou seja, A^h é um ideal principal. Como $(h, k) = 1$, existem inteiros r, s tais que $rh + sk = 1$. Então, como A^k é um ideal principal, segue pelo item 5 da Proposição 6 que:

$$A = A^{rh+sk} = (A^h)^r (A^k)^s$$

também é um ideal principal. □

Vimos, anteriormente, a definição da norma de um ideal de O_K, sendo K um corpo de números algébricos. Estenderemos agora esta definição para ideais fracionários, e apresentaremos, sem demonstrar, uma propriedade.

Definição 74 (Norma de um ideal fracionário)**.** *Sejam K um corpo de números algébricos, O_K o seu anel de inteiros e A um ideal fracionário não-nulo de O_K. Então existe um ideal não-nulo I de O_K e um elemento não-nulo $\alpha \in O_K$ tais que:*

$$A = \frac{1}{\alpha} I$$

Definimos a norma $N(A)$ do ideal fracionário A como sendo:

$$N(A) = \frac{N(I)}{N(\langle \alpha \rangle)}$$

em que $N(I)$ e $N(\langle \alpha \rangle)$ são as normas dos ideais I e $\langle \alpha \rangle$.

Mostremos que definição anterior é válida. Para isso, faremos uso do seguinte resultado:

Teorema 105. *Sejam K um corpo de números algébricos e A e B ideais de O_K. Então:*

$$N(AB) = N(A)N(B)$$

Sejam I e J ideais não-nulos de O_K e $\alpha, \beta \in O_K$ tais que:

$$\frac{1}{\alpha} I = \frac{1}{\beta} J$$

Então:

$$\beta I = \alpha J$$

de forma que vale a igualdade entre os produtos:

$$\langle \beta \rangle \, I = \langle \alpha \rangle \, J$$

Assim, pelo Teorema 105, temos:

$$N(\langle \beta \rangle) N(I) = N(\langle \beta \rangle \, I) = N(\langle \alpha \rangle \, J) = N(\langle \alpha \rangle) N(J)$$

donde:

$$\frac{N(I)}{N(\langle \alpha \rangle)} = \frac{N(J)}{N(\langle \beta \rangle)}$$

Assim, a norma de um ideal fracionário está bem definida. Ainda, note que se A é um ideal de O_K, então a definição da norma de A vista como a norma de um ideal fracionário coincide com a definição da norma de A como um ideal de O_K. De fato, se $N'(A)$ é a norma de A considerando A um ideal fracionário de O_K e $N(A)$ é a norma de A considerado como um ideal de O_K, temos:

$$N'(A) = \frac{N(A)}{N(\langle 1 \rangle)} = N(A)$$

uma vez que A é ideal de O_K.

Apresentaremos então o resultado de nosso interesse, generalizando o Teorema 105.

Teorema 106. *Sejam K um corpo de números algébricos, O_K o seu anel de inteiros, A e B ideais fracionários de O_K. Então:*

$$N(AB) = N(A)N(B)$$

Demonstração. Como A e B são ideais fracionários não-nulos de O_K, existem ideais não-nulos I e J de O_K e $\alpha, \beta \in O_K \setminus \{0\}$ tais que:

$$A = \frac{1}{\alpha} I \text{ e } B = \frac{1}{\beta} J$$

Então:

$$AB = \frac{1}{\alpha\beta} IJ$$

De forma que:

$$\begin{aligned} N(AB) &= \frac{N(IJ)}{N(\langle\alpha\beta\rangle)} = \\ &= \frac{N(IJ)}{N(\langle\alpha\rangle\langle\beta\rangle)} = \\ &= \frac{N(I)N(J)}{N(\langle\alpha\rangle)N(\langle\beta\rangle)} (\text{pelo Teorema 105}) = \\ &= \frac{N(I)}{N(\langle\alpha\rangle)} \times \frac{N(J)}{N(\langle\beta\rangle)} = \\ &= N(A)N(B) \end{aligned}$$

□

Por fim, apresentaremos, sem demonstrar, um resultado, no qual definiremos a unidade fundamental de O_K com K corpo de números algébricos.

Teorema 107. *Seja m um inteiro positivo livre de quadrados. Então existe uma unidade $\nu > 1$ de $O_{\mathbb{Q}(\sqrt{m})}$ tal que toda unidade de $O_{\mathbb{Q}(\sqrt{m})}$ é da forma $\pm\nu^n$, com $n \in \mathbb{Z}$. Ainda, esta unidade ν é única e é a menor unidade de $O_{\mathbb{Q}(\sqrt{m})}$ maior que 1. A esta unidade damos o nome de unidade fundamental de $\mathbb{Q}(\sqrt{m})$. Se $O_{\mathbb{Q}(\sqrt{m})}$ contém unidades de norma -1, estas são dadas por $\pm\nu^{2n+1}$ e as unidades de norma 1 são dadas por $\pm\nu^{2n}$, com $n \in \mathbb{Z}$. Neste caso, a unidade fundamental de norma 1 é dada por ν^2.*

Note ainda que, se m é um inteiro negativo livre de quadrados, já sabíamos encontrar as unidades de $O_{\mathbb{Q}(\sqrt{m})}$, donde o resultado anterior nos permite terminar de caracterizar as unidades para os anéis de inteiros de corpos de números algébricos.

7.2 A EQUAÇÃO $y^2 = x^3 + k$

Analisaremos alguns casos da equação $y^2 = x^3 + k$, e utilizaremos dos resultados estabelecidos ao longo do texto para verificar se a equação em questão possui ou não soluções, além de encontrá-las em alguns casos.

Primeiramente, usaremos da teoria elementar dos números para mostrar que, para certos valores de k, essa equação não possui solução.

Teorema 108. *Sejam M e N inteiros tais que:*

$$M \equiv 3 \pmod 4 \text{ e } N \equiv 2 \pmod 4$$

sendo que todos os divisores primos p de $\dfrac{N}{2}$ satisfazem $p \equiv 1 \pmod 4$. Então, se $k = M^3 - N^2$, a equação $y^2 = x^3 + k$ não possui soluções inteiras.

Demonstração. Suponha que $(x, y) \in \mathbb{Z}^2$ é uma solução de $y^2 = x^3 + k$. Como $k \equiv M^3 - N^2 \equiv 27 - 4 \equiv -1 \pmod 4$, temos:

$$y^2 \equiv x^3 - 1 \pmod 4$$

Como $y^2 \equiv 0, 1 \pmod 4$ para todo $y \in \mathbb{Z}$, a relação acima não pode ser satisfeita se $x \equiv 0, 2, 3 \pmod 4$. Assim, devemos ter $x \equiv 1 \pmod 4$. Como $k = M^3 - N^2$, vemos que:

$$y^2 + N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

Como $x \equiv 1 \pmod 4$ e $M \equiv 3 \pmod 4$, segue que:

$$x^2 - Mx + M^2 \equiv 3 \pmod 4$$

Então $x^2 - Mx + M^2$ é ímpar e a relação acima mostra que esta expressão possui ao menos um fator primo $p \equiv 3 \pmod 4$. Assim, $y^2 \equiv -N^2 \pmod p$. Por hipótese, temos $p \nmid N$. Logo:

$$\left(\frac{-1}{p}\right) = \left(\frac{-N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

o que contradiz $p \equiv 3 \pmod 4$. Portanto, a equação não possui soluções inteiras. □

Abaixo, seguem alguns valores de M, N e k para os quais a equação $y^2 = x^3 + k$ não possui soluções inteiras usando o resultado anterior.

M	-1	15	3	3
N	2	58	2	10
k	-5	11	23	-73

Teorema 109. *Sejam M e N inteiros tais que:*

$$M \equiv 2 \pmod 4 \text{ e } N \equiv 1 \pmod 2$$

com os divisores primos p de N satisfazendo $p \equiv 1 \pmod 4$. Então a equação $y^2 = x^3 + k$ não tem solução inteira.

Demonstração. Suponha que $(x, y) \in \mathbb{Z}^2$ é uma solução de $y^2 = x^3 + k$. Considerando a equação módulo 4, obtemos:

$$y^2 \equiv x^3 - 1 \pmod 4$$

Então, devemos ter $x \equiv 1 \pmod 4$. Como $k = M^3 - N^2$, temos:

$$y^2 + N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

Uma vez que $x \equiv 1 \pmod 4$ e $M \equiv 2 \pmod 4$, obtemos:

$$x^2 - Mx + M^2 \equiv 3 \pmod 4$$

Pelas mesmas considerações feitas ao final do Teorema 108, o resultado segue. □

Abaixo, seguem alguns valores de M, N e k para os quais a equação $y^2 = x^3 + k$ não possui soluções inteiras usando o resultado anterior.

M	2	-2	2	-2	6	14	6
N	1	1	5	5	13	53	17
k	7	-9	-17	-33	47	-65	-73

Teorema 110. *Sejam M e N inteiros tais que:*

$$M \equiv 4, 6 \pmod 8 \text{ e } N \equiv 1 \pmod 2$$

com todos os divisores primos p de N sendo da forma $p \equiv \pm 1 \pmod 8$. Seja $k = M^3 + 2N^2$. Então a equação $y^2 = x^3 + k$ não tem solução inteira.

Demonstração. Suponha que $(x, y) \in \mathbb{Z}^2$ é uma solução de $y^2 = x^3 + k$. Como $k = M^3 + 2N^2 \equiv 2 \pmod 4$, temos:

$$y^2 \equiv x^3 + 2 \pmod 4$$

Então $x \not\equiv 0 \pmod 2$ e $x \not\equiv 1 \pmod 4$, donde $x \equiv 3 \pmod 4$. Ainda, temos:

$$y^2 - 2N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

Se $x \equiv 3 \pmod 8$, então:

$$x^2 - Mx + M^2 \equiv 1 - 3M + M^2 \equiv \pm 3 \pmod 8$$

Logo $x^2 - Mx + M^2$ é ímpar e pelo menos um de seus fatores primos p é tal que $p \equiv \pm 3 \pmod 8$. Logo, $p \nmid N$ e $y^2 \equiv 2N^2 \pmod p$, donde:

$$\left(\frac{2}{p}\right) = \left(\frac{2N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

contradizendo $p \equiv \pm 3 \pmod 8$.

Se $x \equiv 7 \pmod 8$, então:

$$x + M \equiv 7 + M \equiv \pm 3 \pmod 8$$

Então $x + M$ é ímpar e pelo menos um de seus fatores primos p satisfaz $p \equiv \pm 3 \pmod 8$. Logo, $p \nmid N$ e $y^2 \equiv 2N^2 \pmod p$, donde:

$$\left(\frac{2}{p}\right) = \left(\frac{2N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

contradizendo $p \equiv \pm 3 \pmod 8$.

Com isso, segue que $y^2 = x^3 + k$ não possui soluções inteiras. □

Abaixo, seguem alguns valores de M, N e k para os quais a equação $y^2 = x^3 + k$ não possui soluções inteiras usando o resultado anterior.

M	-2	-4	-10	-4	4	2
N	1	7	23	1	1	7
k	-6	34	58	-62	66	90

Teorema 111. *Sejam M e N inteiros tais que:*

$$M \equiv 4 \pmod 8 \text{ e } N \equiv 1 \pmod 2$$

com todos os divisores primos p de N satisfazendo $p \equiv 1, 3 \pmod 8$. Defina $k = M^3 - 2N^2$. Então, a equação $y^2 = x^3 + k$ não possui soluções inteiras.

Demonstração. Suponha que $(x, y) \in \mathbb{Z}^2$ é uma solução de $y^2 = x^3 + k$. Como $k = M^3 - 2N^2 \equiv 2 \pmod 4$, temos:

$$y^2 \equiv x^3 + 2 \pmod 4$$

Então devemos ter $x \equiv 3 \pmod 4$. Ainda, como $k \equiv -2 \pmod 8$, temos:

$$y^2 \equiv x^3 - 2 \pmod 8$$

donde $x \not\equiv 7 \pmod 8$. Então, $x \equiv 3 \pmod 8$. Note que:

$$y^2 + 2N^2 = x^3 + M^3 = (x + M)(x^2 - Mx + M^2)$$

Como $x \equiv 3 \pmod 8$ e $M \equiv 4 \pmod 8$, temos que $x + M \equiv 7 \pmod 8$. Então $x + M$ é ímpar e tem ao menos um fator primo da forma $p \equiv 5, 7 \pmod 8$. Assim, $p \nmid N$, $y^2 \equiv -2N^2 \pmod p$ e:

$$\left(\frac{-2}{p}\right) = \left(\frac{-2N^2}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

contradizendo $p \equiv 5$ ou $7 \pmod 8$. □

Abaixo, seguem alguns valores de M, N e k para os quais a equação $y^2 = x^3 + k$ não possui soluções inteiras usando o resultado anterior.

M	4	4	-4	-4	4
N	3	1	1	3	9
k	46	62	-66	-82	-98

Note que este método apenas nos diz quando uma equação desta forma não tem solução. Se k é um inteiro que não é coberto por nenhum dos resultados anteriores, não conseguimos determinar se existem ou não soluções e, caso existam, não temos um método para encontrá-las. Para fazermos o estudo para outros valores de k e encontrarmos soluções, usaremos agora dos resultados referentes à teoria algébrica dos números (em particular, à fatoração em ideais). Antes, entretanto, provaremos um resultado importante.

Teorema 112. *Sejam D um domínio de Dedekind e A, B e C ideais não-nulos de D tais que A e B são coprimos e:*

$$AB = C^n$$

com n inteiro positivo. Então, existem ideais A_1 e B_1 de D tais que:

$$A = A_1^n, B = B_1^n, C = A_1B_1$$

Demonstração. Como D é um domínio de Dedekind, todo ideal não-nulo de D pode ser expresso unicamente como um produto de ideais primos de D (pelo Teorema 95). Então:

$$C = P_1^{a_1}...P_r^{a_r}$$

em que $r > 0$ e $P_1, ..., P_r$ são ideais primos distintos de D e $a_1, ..., a_r$ são inteiros positivos. Então:

$$AB = P_1^{na_1}...P_r^{na_r}$$

Como A e B são ideais coprimos, cada potência de ideal $P_i^{na_i}$ divide apenas um dentre A e B (com $i \in \{1, ..., r\}$). Reordenando os índices se necessário, temos:

$$A = P_1^{na_1}...P_s^{na_s} \text{ e } B = P_{s+1}^{na_{s+1}}...P_r^{na_r}$$

para algum inteiro s com $0 < s \leq r$. Sejam $A_1 = P_1^{a_1}...P_s^{a_s}$ e $B_1 = P_{s+1}^{a_{s+1}}...P_r^{a_r}$. Então $A = A_1^n$, $B = B_1^n$ e $C = A_1B_1$. □

Teorema 113. *Seja k um inteiro tal que:*

$$k < -1$$
$$k \text{ é livre de quadrados}$$
$$k \equiv 2, 3 \pmod 4$$
$$h(\mathbb{Q}(\sqrt{k})) \not\equiv 0 \pmod 3$$

1. *Se existe um inteiro a tal que:*

   $$k = 1 - 3a^2$$

   Então as únicas soluções inteiras de $y^2 = x^3 + k$ são:

   $$x = 4a^2 - 1, y = \pm(3a - 8a^3)$$

2. *Se existe um inteiro a tal que:*

   $$k = -1 - 3a^2$$

   então as únicas soluções inteiras de $y^2 = x^3 + k$ são:

   $$x = 4a^2 - 1, y = \pm(3a - 8a^3)$$

3. Se $k \neq \pm 1 - 3a^2$ para algum inteiro a então $y^2 = x^3 + k$ não possui soluções inteiras.

Demonstração. Primeiramente, note que no item 1, $k \equiv 1 \pmod 3$ e no item 2, $k \equiv 2 \pmod 3$, donde os casos nos itens 1 e 2 são disjuntos. Suponha que $y^2 = x^3 + k$ tem uma solução inteira. Primeiramente, mostremos que $x \equiv 1 \pmod 2$. Como $y^2 \equiv 0, 1 \pmod 4$ e $k \equiv 2, 3 \pmod 4$, vemos que $x^3 = y^2 - k \equiv 1, 2, 3 \pmod 4$. Mas $x^3 \not\equiv 2 \pmod 4$, donde $x \equiv 1 \pmod 2$.

Suponha que $(x, k) \neq 1$. Então existe um primo p tal que $p \mid x$ e $p \mid k$. Como k é livre de quadrados, temos $p \| k$. Então, $p \| x^3 + k$ e então $p \| y^2$, um absurdo. Logo, $(x, k) = 1$.

De $x \equiv 1 \pmod 2$ e $(x, k) = 1$ deduzimos que $(x, 2k) = 1$, donde existem inteiros l e m tais que:

$$lx + m(2k) = 1$$

Seja $K = \mathbb{Q}(\sqrt{k})$ um corpo quadrático imaginário. Como $k \equiv 2, 3 \pmod 4$, sabemos que o anel de inteiros O_K de K é $\mathbb{Z} + \mathbb{Z}\sqrt{k}$. Mostremos agora que os ideais $\left\langle y + \sqrt{k} \right\rangle$ e $\left\langle y - \sqrt{k} \right\rangle$ de O_K são coprimos. Suponha que isso seja falso. Então existe um ideal primo P tal que:

$$P \mid \left\langle y + \sqrt{k} \right\rangle, \left\langle y - \sqrt{k} \right\rangle$$

Donde:

$$y + \sqrt{k}, y - \sqrt{k} \in P$$

Então:

$$2\sqrt{k} = (y + \sqrt{k}) - (y - \sqrt{k}) \in P$$

e

$$2k = \sqrt{k}(2\sqrt{k}) \in P$$

Como $\left\langle y + \sqrt{k} \right\rangle \left\langle y - \sqrt{k} \right\rangle = \langle y^2 - k \rangle = \langle x^3 \rangle = \langle x \rangle^3$, temos $P \mid \langle x \rangle^3$, donde $P \mid \langle x \rangle$ e $x \in P$. Dessa forma, $1 = lx + m(2k) \in P$, o que é absurdo, pois $1 \in P$ implica em $P = D$, o que contradiz P ser primo.

Logo, $\left\langle y + \sqrt{k} \right\rangle$ e $\left\langle y - \sqrt{k} \right\rangle$ são ideais coprimos de O_K com $\left\langle y + \sqrt{k} \right\rangle \left\langle y - \sqrt{k} \right\rangle = \langle x \rangle^3$. Como K é um corpo de números algébricos, O_K é um domínio de Dedekind pelo Teorema 90, e então pelo Teorema 112 existe um ideal A de O_K tal que:

$$\left\langle y + \sqrt{k} \right\rangle = A^3$$

Então A^3 é um ideal principal e, como $h(\mathbb{Q}(\sqrt{k})) = h(K) \not\equiv 0 \pmod 3$, segue pelo Teorema 104 que A é um ideal principal. Assim, existem $a, b \in \mathbb{Z}$ tais que:

$$A = \left\langle a + b\sqrt{k} \right\rangle$$

Então:

$$\left\langle y + \sqrt{k} \right\rangle = \left\langle a + b\sqrt{k} \right\rangle^3 = \left\langle (a + b\sqrt{k})^3 \right\rangle$$

Pelo Teorema 2, existe uma unidade $u \in O_K$ tal que:

$$y + \sqrt{k} = u(a + b\sqrt{k})^3 \tag{7.1}$$

Sabemos que $u = a' + b'\sqrt{k}$ com $a', b' \in \mathbb{Z}$ e $u \mid 1$. Como $k < -1$ e $k \equiv 2, 3 \pmod 4$, segue pela função ϕ_k que:

$$a'^2 - kb'^2 = 1$$

Se $b' \neq 0$, então $a'^2 - kb'^2 \geq a'^2 - k > a'^2 + 1 \geq 1$, o que é um absurdo. Então $b' = 0$ e $a'^2 = 1$, donde $a' = u = \pm 1$. Tomando o conjugado na equação (7.1), obtemos:

$$y - \sqrt{k} = u(a - b\sqrt{k})^3 \tag{7.2}$$

Assim:

$$x^3 = y^2 - k = (y+\sqrt{k})(y-\sqrt{k}) = (a+b\sqrt{k})^3(a-b\sqrt{k})^3 = ((a+b\sqrt{k})(a-b\sqrt{k}))^3 = (a^2-kb^2)^3$$

de forma que:

$$x = a^2 - kb^2$$

Adicionando e subtraindo as equações (7.1) e (7.2), encontramos:

$$2y = u((a + b\sqrt{k})^3 + (a - b\sqrt{k})^3)$$

e

$$2\sqrt{k} = u((a + b\sqrt{k})^3 - (a - b\sqrt{k})^3)$$

de forma que $y = u(a^3 + 3kab^2)$ e $1 = u(3a^2b + kb^3)$. Dessa última igualdade, vemos que $b \mid 1$, donde $b = \pm 1 = \pm u$. Se $b = u$, temos:

$$x = a^2 - k, y = u(a^3 + 3ka), 1 = 3a^2 + k$$

de forma que:

$$k = 1 - 3a^2$$

e $x = 4a^2 - 1$, $y = \pm(3a - 8a^3)$. Note que ainda temos que mostrar que estas são, de fato, soluções, pois até agora mostramos apenas que se existissem soluções, estas deveriam ser dessa forma. Tal verificação, entretanto, é direta, pois:

$$x^3 + k = (4a^2 - 1)^3 + (1 - 3a^2) = 64a^6 - 48a^4 + 9a^2 = (8a^3 - 3a)^2 = y^2$$

Donde o item 1 segue.

Se $b = -u$, então:

$$x = a^2 - k, y = u(a^3 + 3ka), 1 = -3a^2 - k$$

donde:

$$k = -1 - 3a^2$$

e $x = 4a^2 + 1$, $y = \pm(3a + 8a^3)$. Ainda, vale que:

$$x^3 + k = (4a^2 + 1)^3 - 1 - 3a^2 = 64a^6 + 48a^4 + 9a^2 = (8a^3 + 3a)^2 = y^2$$

Donde o item 2 segue.

Por fim, se $k \neq \pm 1 - 3a^2$ para todo $a \in \mathbb{Z}$, então $b \neq -1, 1$ (pois vimos que $b = \pm 1$ implica em $k = \pm 1 - 3a^2$), o que é um absurdo, pois mostramos que $b \mid 1$. Assim, o item 3 segue. □

O resultado anterior nos permite analisar a equação $y^2 = x^3 + k$ para grande parte dos casos em que $k < 0$. Mostraremos agora alguns resultados referentes a $k > 0$.

Teorema 114. *Seja k um inteiro tal que:*

$$k > 0$$
$$k \text{ é livre de quadrados}$$
$$k \equiv 2, 3 \pmod 4$$
$$h(\mathbb{Q}(\sqrt{k})) \not\equiv 0 \pmod 3$$

Seja $T + U\sqrt{k}$ a unidade fundamental de $K = \mathbb{Q}(\sqrt{k})$ de norma 1. Se uma das opções:

$$k \equiv 4 \pmod 9 \text{ e } U \equiv 0 \pmod 9$$
$$k \equiv 7 \pmod 9 \text{ e } U \equiv \pm 3 \pmod 9$$
$$k \equiv 4 \pmod 7 \text{ e } U \equiv 0 \pmod 7$$

ocorre, então a equação $y^2 = x^3 + k$ não tem soluções inteiras.

Demonstração. Prosseguindo como na demonstração do Teorema 113, obtemos:

$$y + \sqrt{k} = u(a + b\sqrt{k})^3$$

em que $a, b \in \mathbb{Z}$ e u é uma unidade de O_K, com $K = \mathbb{Q}(\sqrt{k})$. Seja ν a unidade fundamental de O_K, de forma que:

$$u = \pm\nu^l$$

com $l \in \mathbb{Z}$. Como os cubos $-1 = (-1)^3$ e $\nu^{3m} = (\nu^m)^3$ podem ser absorvidos no cubo $(a + b\sqrt{k})^3$, temos $y + \sqrt{k} = u(a + b\sqrt{k})^3$, em que $u = 1, \nu$ ou ν^2. Ainda, como $\nu = \dfrac{\nu^3}{\nu^2}$ e $\nu^2 = \dfrac{\nu^3}{\nu}$ e os cubos podem ser absorvidos, temos:

$$y + \sqrt{k} = u(a + b\sqrt{k})^3, \text{ com } u \in \left\{1, \nu, \frac{1}{\nu}\right\} \text{ ou } \left\{1, \frac{1}{\nu^2}, \nu^2\right\}$$

Escolhamos $u \in \left\{1, \nu, \dfrac{1}{\nu}\right\}$ se ν tiver norma 1 e $u \in \left\{1, \dfrac{1}{\nu^2}, \nu^2\right\}$ se ν tiver norma -1. Em ambos os casos, temos:

$$u \in \{1, T + U\sqrt{k}, T - U\sqrt{k}\}$$

em que $T + U\sqrt{k}$ é a unidade fundamental (> 1) de O_K de norma 1. Se $u = 1$, igualando os coeficientes de $\sqrt{k}$, obtemos $1 = 3a^2b + kb^3$, de forma que $b \mid 1$ e $b = \pm 1$. Então $\pm 1 = b = 3a^2b^2 + kb^4 = 3a^2 + k \geq k > 1$, um absurdo. Logo, $u = T \pm U\sqrt{k}$. Assim:

$$\begin{aligned} y + \sqrt{k} &= (T \pm U\sqrt{k})(a + b\sqrt{k})^3 = \\ &= (T \pm U\sqrt{k})((a^3 + 3kab^2) + (3a^2b + kb^3)\sqrt{k}) = \\ &= (T(a^3 + 3kab^2) \pm Uk(3a^2b + kb^3)) + (T(3a^2b + kb^3) \pm U(a^3 + 3kab^2))\sqrt{k} \end{aligned}$$

donde:

$$1 = T(3a^2b + kb^3) \pm U(a^3 + 3kab^2) \tag{7.3}$$

Temos os seguintes casos:

1. Caso $k \equiv 4 \pmod 9$ e $U \equiv 0 \pmod 9$: Como $U \equiv 0 \pmod 9$, de $T^2 - kU^2 = 1$ obtemos que $T \equiv \pm 1 \pmod{81}$, assim:

   $$T \equiv \epsilon \pmod{81}, \text{ com } \epsilon \in \{-1, 1\}$$

   Pela equação (7.3) módulo 9, encontramos:

   $$1 \equiv \epsilon(3a^2b + 4b^3) \pmod 9 \tag{7.4}$$

   Essa congruência implica em $b \not\equiv 0 \pmod 3$. Então $b \equiv \lambda \pmod 3$ com $\lambda \in \{-1, 1\}$. Logo:

   $$b^3 \equiv \lambda \pmod 9$$

   Então, pela equação (7.4), deduzimos que:

   $$1 \equiv \epsilon\lambda(3a^2 + 4) \pmod 9$$

   de forma que:

   $$3a^2 + 4 \equiv \epsilon\lambda \equiv \pm 1 \pmod 9$$

   Assim:

   $$3a^2 \equiv 4 \text{ ou } 6 \pmod 9$$

   e ambos os casos são impossíveis.

2. Caso $k \equiv 7 \pmod 9$ e $U \equiv \pm 3 \pmod 9$: Neste caso, $U^2 \equiv 0 \pmod 9$. De $T^2 - kU^2 = 1$ deduzimos que $T^2 \equiv 1 \pmod 9$, donde:

   $$T \equiv \epsilon \pmod 9, \text{ com } \epsilon \in \{-1, 1\}$$

   Ainda, pela equação (7.3) módulo 3, obtemos:

   $$1 \equiv \epsilon b^3 \pmod 3$$

de forma que:

$$b \equiv \epsilon \pmod 3 \text{ e } b^3 \equiv \epsilon \pmod 9$$

Então, de (7.3) módulo 9, temos:

$$1 \equiv 3a^2 + 7 \pm 3a^3 \pmod 9$$

Tal fato implica que $a \not\equiv 0 \pmod 3$, de forma que $a \equiv \pm 1 \pmod 3$, $a^2 \equiv 1 \pmod 3$ e $a^3 \equiv a \pmod 3$. Então:

$$1 \equiv 1 \pm 3a \pmod 9$$

o que nos dá $a \equiv 0 \pmod 3$, um absurdo.

3. Caso $k \equiv 4 \pmod 7$ e $U \equiv 0 \pmod 7$: Da equação:

$$y + \sqrt{k} = (T \pm U\sqrt{k})(a + b\sqrt{k})^3$$

deduzimos que:

$$y - \sqrt{k} = (T \mp U\sqrt{k})(a - b\sqrt{k})^3$$

donde:

$$\begin{aligned} x^3 = y^2 - k &= (y + \sqrt{k})(y - \sqrt{k}) = \\ &= (T \pm U\sqrt{k})(a + b\sqrt{k})^3(T \mp U\sqrt{k})(a - b\sqrt{k})^3 = \\ &= (T^2 - kU^2)(a^2 - kb^2)^3 = \\ &= (a^2 - kb^2)^3 \end{aligned}$$

e então:

$$x = a^2 - kb^2$$

Como:

$$x^3 \equiv 0, 1, 6 \pmod 7$$

e

$$y^2 \equiv 0, 1, 2, 4 \pmod 7$$

temos:

$$y^2 - x^3 = k \equiv 4 \pmod 7$$

Assim:

$$y^2 \equiv 4 \pmod 7 \text{ e } x^3 \equiv 0 \pmod 7$$

Então:

$$x \equiv 0 \pmod 7$$

donde:

$$a^2 - 4b^2 \equiv 0 \pmod 7$$

ou seja:

$$a \equiv \pm 2b \pmod 7$$

De $U \equiv 0 \pmod 7$ e $T^2 - kU^2 = 1$, deduzimos:

$$T^2 \equiv 1 \pmod{49}$$

donde:

$$T \equiv \pm 1 \pmod{49}$$

Então, da equação (7.3), obtemos:

$$1 \equiv \pm 2b^3 \pmod 7$$

o que é impossível.

Com isso, vemos que $y^2 = x^3 + k$ é insolúvel nos inteiros em todos os 3 casos. □

Por fim, mostraremos um caso quando $h(\mathbb{Q}(\sqrt{k})) \equiv 0 \pmod 3$. Usaremos, sem provar, o fato que $h(\mathbb{Q}(\sqrt{-31})) = 3$ (esse resultado pode ser encontrado em (1)).

Teorema 115. *A equação:*

$$y^2 = x^3 - 31 \tag{7.5}$$

não tem soluções inteiras.

Demonstração. Suponha que $y^2 = x^3 - 31$ tem uma solução inteira (x, y). Notemos que $31 \nmid y$, pois se $31 \mid y$ então $31 \mid x$ e assim $31^2 \mid x^3 - y^2 = 31$, o que é um absurdo.

Mostraremos agora que x deve ser par. Suponha que x é ímpar. Se $x \equiv 1 \pmod 4$ então $x^3 \equiv 1 \pmod 4$ e assim $y^2 \equiv x^3 - 31 \equiv 2 \pmod 4$, o que é um absurdo. Se $x \equiv 3 \pmod 4$ então $x^2 + 3x + 9 \equiv 3 \pmod 4$. Ainda, $x^2 + 3x + 9 > 1$ (pois esta desigualdade vale para todo $x \in \mathbb{R}$). Então, $x^2 + 3x + 9$ tem um fator primo p com $p \equiv 3 \pmod 4$. Assim:

$$y^2 + 4 = x^3 - 27 = (x - 3)(x^2 + 3x + 9)$$

de forma que $y^2 + 4 \equiv 0 \pmod p$, o que é impossível, pois:

$$-1 = \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{4}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{y^2}{p}\right) = 1$$

o que é um absurdo. Logo, x é par e y é ímpar.

Usaremos, sem provar, o fato que $\left\{1, \dfrac{1 + \sqrt{-31}}{2}\right\}$ é uma base inteira para $K = \mathbb{Q}(\sqrt{-31})$ (esse resultado pode ser encontrado em (1)). Uma fatoração em ideais primos de 2 em O_K é dada por:

$$\langle 2 \rangle = \left\langle 2, \frac{3 + \sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{3 - \sqrt{-31}}{2} \right\rangle \tag{7.6}$$

Mostremos que $\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle$ não é um ideal principal. Suponha que seja. Então, existem $a, b \in \mathbb{Z}$ tais que:

$$\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle = \left\langle a + b\left(\frac{1+\sqrt{-31}}{2}\right) \right\rangle$$

Tomando as normas dos ideais, temos:

$$2 = N\left(\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle\right) = N\left(\left\langle a + b\left(\frac{1+\sqrt{-31}}{2}\right) \right\rangle\right) =$$
$$= \left| N\left(\frac{2a+b+b\sqrt{-31}}{2}\right) \right| = \frac{(2a+b)^2 + 31b^2}{4}$$

De forma que:

$$(2a+b)^2 + 31b^2 = 8$$

o que é impossível.

Usando das equações (7.5) e (7.6), deduzimos que:

$$\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = \left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle \left\langle 2, \frac{3-\sqrt{-31}}{2} \right\rangle \left\langle \frac{x}{2} \right\rangle^3 \tag{7.7}$$

Mostremos que os ideais $\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle$ e $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$ são coprimos. Suponha o contrário. Então, existe um ideal primo P tal que:

$$P \mid \left\langle \frac{y+\sqrt{-31}}{2} \right\rangle, \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$$

Assim:

$$\frac{y+\sqrt{-31}}{2}, \frac{y-\sqrt{-31}}{2} \in P$$

donde:

$$\sqrt{-31} = \frac{y+\sqrt{-31}}{2} - \frac{y-\sqrt{-31}}{2} \in P$$

Então:

$$P \mid \left\langle \sqrt{-31} \right\rangle$$

Mas P e $\left\langle \sqrt{-31} \right\rangle$ são ambos ideais primos, de forma que:

$$P = \left\langle \sqrt{-31} \right\rangle$$

Portanto:

$$\left\langle \sqrt{-31} \right\rangle \mid \left\langle \frac{y+\sqrt{-31}}{2} \right\rangle$$

donde segue que $\frac{y+\sqrt{-31}}{2} \in \left\langle \sqrt{-31} \right\rangle$. Isso mostra que existem inteiros u e v tais que:

$$\frac{y+\sqrt{-31}}{2} = \sqrt{-31}\left(\frac{u+v\sqrt{-31}}{2}\right)$$

Assim, $u = 1$ e $y = -31v$, o que contradiz $31 \nmid y$. Isso mostra que os ideais $\left\langle \frac{y+\sqrt{-31}}{2} \right\rangle$ e $\left\langle \frac{y-\sqrt{-31}}{2} \right\rangle$ são coprimos. Substituindo y por $-y$ se necessário, vemos de (7.7) que existe um ideal A de O_K tal que:

$$\begin{cases} \left\langle \frac{y+\sqrt{-31}}{2} \right\rangle = \left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle A^3 \\ \left\langle \frac{y-\sqrt{-31}}{2} \right\rangle = \left\langle 2, \frac{3-\sqrt{-31}}{2} \right\rangle \overline{A}^3 \\ \left\langle \frac{x}{2} \right\rangle = A\overline{A} \end{cases}$$

em que $\overline{A} = \{\overline{a} \mid a \in A\}$ denota o ideal conjugado de A. Como $h(\mathbb{Q}(\sqrt{-31})) = 3$ o ideal A^3 é principal. Da primeira equação do sistema acima, deduzimos que o ideal $\left\langle 2, \frac{3+\sqrt{-31}}{2} \right\rangle$ é principal, o que é um absurdo. Com isso, vemos que a equação $y^2 = x^3 - 31$ não tem soluções inteiras. □

7.3 A EQUAÇÃO $y(y+1) = x(x+1)(x+2)$

Nesta seção, usaremos o corpo cúbico $K = \mathbb{Q}(\theta)$, com θ satisfazendo $\theta^3 - 4\theta + 2 = 0$. Para isso, usaremos, sem provar, os seguintes resultados sobre K (os quais podem ser encontrados em (1)):

$$O_K = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 \tag{7.8}$$

$$O_K \text{ é um domínio de fatoração única} \tag{7.9}$$

$$\{\epsilon, \nu\} \text{ é um sistema fundamental de unidades de } O_K, \text{ com } \epsilon = \theta - 1 \text{ e } \nu = 2\theta - 1 \tag{7.10}$$

$$\text{Toda unidade de } O_K \text{ é dada por } \pm\epsilon^m\nu^n \text{ com } m, n \in \mathbb{Z} \tag{7.11}$$

Para estudar esta equação, a transformaremos em outro problema. Definamos $X = 2x + 2$ e $Y = 2y + 1$. Então a equação:

$$x(x+1)(x+2) = y(y+1) \tag{7.12}$$

se torna a equação:

$$2Y^2 = X^3 - 4X + 2 \tag{7.13}$$

Se (x, y) é uma solução de (7.12), então a solução (X, Y) de (7.13) correspondente satisfaz X par e Y ímpar.

Sejam $\theta, \theta', \theta'' \in \mathbb{C}$ as raízes de $x^3 - 4x + 2 = 0$. Então:

$$\begin{cases} \theta + \theta' + \theta'' = 0 \\ \theta\theta' + \theta'\theta'' + \theta''\theta = -4 \\ \theta\theta'\theta'' = -2 \end{cases} \tag{7.14}$$

Provaremos agora uma sequência de lemas:

Lema 11. *θ é primo em O_K.*

Demonstração. Das equações (7.14) deduzimos que $|N(\theta)| = |\theta\theta'\theta''| = 2$, o qual é um inteiro primo, donde θ é primo em O_K. □

Lema 12. *$4\theta - 3$ é primo em O_K.*

Demonstração. Pelas equações (7.14), temos:

$$\begin{aligned} N(4\theta-3) &= (4\theta-3)(4\theta'-3)(4\theta''-3) = \\ &= 64\theta\theta'\theta'' - 48(\theta\theta' + \theta'\theta'' + \theta''\theta) + 36(\theta+\theta'+\theta'') - 27 = \\ &= 64(-2) - 48(-4) + 36(0) - 27 = \\ &= -128 + 192 - 27 = \\ &= 37 \end{aligned}$$

o qual é um inteiro primo, donde $4\theta - 3$ é primo em O_K. □

Lema 13. *$2 = \rho\theta^3$, com $\rho \in U(O_K)$.*

Demonstração. De $\theta^3 - 4\theta + 2 = 0$ deduzimos que:

$$\frac{\theta^3}{2} = 2\theta - 1 \in O_K$$

Ainda:

$$N\left(\frac{\theta^3}{2}\right) = \frac{N(\theta)^3}{2} = \frac{(-2)^3}{8} = -1$$

Então:

$$\frac{\theta^3}{2} \in U(O_K)$$

Assim:

$$\frac{2}{\theta^3} \in U(O_K)$$

donde:

$$\frac{2}{\theta^3} = \rho$$

para algum $\rho \in U(O_K)$. □

Lema 14. *Se $(X, Y) \in \mathbb{Z}^2$ é uma solução de (7.13), então:*

$$(X - \theta)(X^2 + \theta X + (\theta^2 - 4)) = \rho\theta^3 Y^2$$

Demonstração. Pelas equações (7.13), $\theta^3 - 4\theta + 2 = 0$ e pelo Lema 13, temos:

$$\begin{aligned}(X-\theta)(X^2+\theta X+(\theta^2-4)) &= X^3 - 4X - \theta^3 + 4\theta = \\ &= X^3 - 4X + 2 = \\ &= 2Y^2 = \\ &= \rho\theta^3 Y^2\end{aligned}$$

□

Lema 15. *Os únicos primos de O_K que possivelmente dividem ambos $X-\theta$ e $X^2+\theta X+(\theta^2-4)$ são θ e $4\theta-3$.*

Demonstração. Seja π um primo de O_K que divide ambos $X-\theta$ e $X^2+\theta X+(\theta^2-4)$. Então π divide:

$$\begin{aligned}(X^2+\theta X+(\theta^2-4)) - (X+2\theta)(X-\theta) = 3\theta^2 - 4 = \frac{3\theta^3-4\theta}{\theta} = \frac{3(4\theta-2)-4\theta}{\theta} = \\ = \frac{8\theta-6}{\theta} = \frac{2}{\theta}(4\theta-3) = \rho(4\theta-3)\theta^2\end{aligned}$$

pela equação $\theta^3 - 4\theta + 2 = 0$ e pelo Lema 13. Como ρ é uma unidade isso mostra que as únicas possibilidades para π são $\pi = \theta$ e $\pi = 4\theta - 3$. □

Lema 16. *θ é um fator comum de $X-\theta$ e $X^2+X\theta+(\theta^2-4)$ tal que $\theta^2 \nmid X-\theta$.*

Demonstração. Pelo Lema 13, temos que $\theta^3 \mid 2$ em O_K. Então, como X é par, deduzimos que $\theta^3 \mid X$ em O_K. Assim, $\theta \mid X$, donde $\theta \mid X-\theta$ e $\theta \mid X^2+X\theta+(\theta^2-4)$. Por fim, como $\theta^2 \mid X$ e $\theta^2 \nmid \theta$, temos $\theta^2 \nmid X-\theta$. □

Com estes lemas, podemos então estudar as soluções da equação (7.13).

Teorema 116. *As soluções inteiras da equação* (7.13) *são:*

$$(X,Y) = (-2,\pm1),(0,\pm1),(2,\pm1),(4,\pm5),(12,\pm29)$$

Demonstração. Definamos um inteiro não-negativo n como sendo:

$$(4\theta-3)^n \mid X-\theta, (4\theta-3)^{n+1} \nmid X-\theta$$

Então, como O_K é domínio de fatoração única, da relação anterior, das relações (7.8) e (7.10) e dos Lemas 14 e 15, deduzimos que:

$$X-\theta = \pm\theta(4\theta-3)^n\epsilon^l\nu^m(a+b\theta+c\theta^2)^2$$

para inteiros l, m, a, b, c. Absorvendo os quadrados no termo $(a+b\theta+c\theta^2)^2$, podemos reescrever a igualdade acima como sendo:

$$X-\theta = \pm\theta(4\theta-3)^N\epsilon^L\nu^M(A+B\theta+C\theta^2)^2$$

com A, B, C inteiros e $L, M, N \in \{0, 1\}$. Tomando a norma de ambos os lados da equação acima, obtemos:

$$X^3 - 4X + 2 = \pm 2 \times 37^N \times Z^2$$

para algum $Z \in \mathbb{Z}$. Como X é par podemos definir $X = 2X_1$, com $X_1 \in \mathbb{Z}$, donde a equação acima pode reescrita como:

$$4X_1^3 - 4X_1 + 1 = \pm 37^N \times Z^2$$

Analisando a equação acima módulo 8, temos:

$$1 \equiv \pm 5^N \pmod 8$$

mostrando que $N \neq 1$. Então, como $N \in \{0, 1\}$, temos $N = 0$. Portanto:

$$X - \theta = \pm\theta\epsilon^L\nu^M(A + B\theta + C\theta^2)^2 \tag{7.15}$$

com $L, M \in \{0, 1\}$. Expandindo o quadrado na expressão anterior e fazendo uso do fato que $\theta^3 = \theta - 2$, temos:

$$X - \theta = \pm\theta\epsilon^L\nu^M((A^2 - 4BC) + (2AB + 8BC - 2C^2)\theta + (2AC + B^2 + 4C^2)\theta^2) \tag{7.16}$$

Consideramos agora 4 possibilidades:

$$(L, M) = (0, 0), (0, 1), (1, 0) \text{ e } (1, 1)$$

1. $(L, M) = (0, 0)$: Neste caso, a equação (7.16) se torna:

   $$X - \theta = \pm\theta((A^2 - 4BC) + (2AB + 8BC - 2C^2)\theta + (2AC + B^2 + 4C^2)\theta^2)$$

   Usando que $\theta^3 = 4\theta - 2$, e igualando os termos em 1, θ e θ^2 em ambos os lados da equação acima, obtemos:

   $$4AC + 2B^2 + 8C^2 = \mp X \tag{7.17}$$
   $$A^2 - 4BC + 4B^2 + 8AC + 16C^2 = \mp 1 \tag{7.18}$$
   $$AB + 4BC - C^2 = 0 \tag{7.19}$$

   Analisando a equação (7.18) módulo 4, vemos que $\mp 1 \equiv 0$ ou $1 \pmod 4$. Assim, as equações acima podem ser reescritas como:

   $$4AC + 2B^2 + 8C^2 = X \tag{7.20}$$
   $$(A + 4C)^2 + 4B^2 - 4BC = 1 \tag{7.21}$$
   $$B(A + 4C) = C^2 \tag{7.22}$$

Quando $B = 0$, a equação (7.22) nos dá $C = 0$. Então, de (7.20) obtemos $X = 0$. Se $B \neq 0$, de (7.21) e (7.22), deduzimos que:

$$\frac{C^4}{B^2} + 4B^2 - 4BC = 1 \tag{7.23}$$

Sabemos que, para todo $x \in \mathbb{R}$, vale que:

$$(x - B)^2 \left((x + B)^2 + 2B^2\right) \geq 0$$

Então:

$$x^4 \geq 4B^3x - 3B^4$$

e assim:

$$\frac{x^4}{B^2} + 4B^2 - 4Bx \geq B^2$$

Tomando $x = C$ na desigualdade acima, e usando de (7.23), deduzimos que:

$$1 \geq B^2$$

De forma que $B = \pm 1$. Então, de (7.23) temos:

$$C^4 + 4 \mp 4C = 1$$

donde $C = \pm 1$. Portanto, de (7.22) obtemos $A = \dfrac{C^2}{B} - 4C = \mp 3$. Por fim, de (7.20), obtemos:

$$X = 2 - 12 + 8 = -2$$

2. $(L, M) = (0, 1)$: Neste caso, (7.15) se torna:

$$X - \theta = \pm\theta(2\theta - 1)(A + B\theta + C\theta^2)^2$$

Multiplicando a equação acima por θ e absorvendo θ^2 no quadrado, obtemos:

$$\mp(X\theta - \theta^2) = (1 - 2\theta)((A^2 - 4BC) + (2AB + 8BC - 2C^2)\theta + (2AC + B^2 + 4C^2)\theta^2)$$

e igualando os coeficientes de $1, \theta$ e θ^2, obtemos:

$$0 = A^2 - 4BC + 4(2AC + B^2 + 4C^2) \tag{7.24}$$

$$\mp X = 2AB + 8BC - 2C^2 - 2(A^2 - 4BC) - 8(2AC + B^2 + 4C^2) \tag{7.25}$$

$$\pm 1 = 2AC + B^2 + 4C^2 - 2(2AB + 8BC - 2C^2) \tag{7.26}$$

De (7.24) vemos que A é par e de (7.26) vemos que B é ímpar. Então, considerando (7.26) módulo 4, vemos que $\pm 1 \equiv 1 \pmod 4$, donde o sinal na terceira equação é positivo (e, consequentemente, na segunda é negativo). Assim, as equações acima se tornam:

$$0 = (A + 4C)^2 + 4B(B - C) \tag{7.27}$$

$$1 = A(2C - 4B) + B^2 - 16BC + 8C^2 \tag{7.28}$$

$$X = 2A^2 + 8B^2 + 34C^2 - 2AB - 16BC + 16AC \tag{7.29}$$

Suponha que $C = 2B$. Então de (7.28) obtemos $B^2 = 1$. Como as soluções (A, B, C) e $(-A, -B, -C)$ nos dão o mesmo valor para X, podemos considerar $B = 1$. Então $C = 2$ e de (7.27) obtemos $(A + 8)^2 = 4$, donde $A \in \{-6, -10\}$. Assim, de (7.29) com $(A, B, C) = (-6, 1, 2)$ obtemos $X = 4$ e com $(A, B, C) = (-10, 1, 2)$ obtemos $X = 12$.

Suponha que $C \neq 2B$. Então, de (7.28) temos:

$$A = \frac{B^2 - 16BC + 8C^2 - 1}{4B - 2C}$$

Assim:

$$A + 4C = \frac{B^2 - 1}{4B - 2C} \tag{7.30}$$

Dessa forma, de (7.27), deduzimos que:

$$\left(\frac{B^2 - 1}{4B - 2C}\right)^2 + 4B(B - C) = 0$$

de forma que:

$$B^4 - 2B^2 + 1 + 16B(2B - C)^2(B - C) = 0$$

Isso mostra que $B \mid 1$, donde $B = \pm 1$. Então, a equação anterior nos dá (como $C \neq 2B$) $C = B = \pm 1$. Assim, de (7.30), obtemos $A = -4C = \mp 4$ e de (7.29) $X = 2$.

3. $(L, M) = (1, 0)$: Neste caso, a equação (7.16) se torna:

$$\mp(X - \theta) = (\theta - \theta^2)((A^2 - 4BC) + (2AB + 8BC - 2C^2)\theta + (2AC + B^2 + 4C^2)\theta^2)$$

Igualando os coeficientes de θ e θ^2, obtemos:

$$\pm 1 = (A^2 - 4BC) + 6(2AC + B^2 + 4C^2) - 4(2AB + 8BC - 2C^2)$$
$$0 = (2AB + 8BC - 2C^2) - (A^2 - 4BC) - 4(2AC + B^2 + 4C^2)$$

A primeira equação nos mostra que A é ímpar e a segunda que A é par, o que é um absurdo.

4. $(L, M) = (1, 1)$: Neste caso, (7.15) se torna:

$$\pm(X - \theta) = \theta(1 - \theta)(1 - 2\theta)(A + B\theta + C\theta^2)^2$$

Multiplicando por θ a expressão acima e absorvendo θ^2 no quadrado, obtemos a expressão:

$$\pm\theta(X - \theta) = (1 - 3\theta + 2\theta^2)((A^2 - 4BC) + (2AB + 8BC - 2C^2)\theta + (2AC + B^2 + 4C^2)\theta^2)$$

Igualando os coeficientes de 1 e θ^2, obtemos:

$$0 = (A^2 - 4BC) + 6(2AC + B^2 + 4C^2) - 4(2AB + 8BC - 2C^2)$$
$$\mp 1 = 9(2AC + B^2 + 4C^2) - 3(2AB + 8BC - 2C^2) + 2(A^2 - 4BC)$$

A primeira equação mostra que A é par e então que B também é par pois $6B^2 \equiv 0 \pmod 4$. A segunda mostra que B é ímpar, o que é um absurdo.

Logo, as soluções no enunciado do teorema são as únicas possíveis. Como os pares (X, Y) listados no enunciado são, de fato, soluções, o teorema segue. □

Como consequência do teorema anterior e da transformação feita no começo da seção, obtemos as soluções da equação $y(y+1) = x(x+1)(x+2)$.

Teorema 117. *As soluções inteiras da equação:*

$$y(y+1) = x(x+1)(x+2)$$

são:

$$(x, y) = (0, 0), (0, -1), (-1, 0), (-1, -1), (-2, 0), (-2, -1), (1, 2), (1, -3), (5, 14), (5, -15)$$

7.4 A EQUAÇÃO $x^2 + y^2 = z^2$

Nos resultados das seções anteriores, estudamos apenas equações com duas variáveis e utilizamos de toda a teoria construída ao longo do texto para fazer a análise de suas possíveis soluções. É possível, entretanto, estudar equações diofantinas com mais de duas variáveis com os métodos que desenvolvemos ao longo do texto. Em particular, mostraremos que conseguimos resolver o problema de encontrar as ternas pitagóricas (o qual é um dos mais famosos no estudo de equações diofantinas) utilizando apenas a teoria desenvolvida nos primeiros capítulos (isto é, fazendo uso apenas de domínios Euclidianos, de ideais principais e de fatoração única). Para isso, daremos duas demonstrações do mesmo resultado, uma delas utilizando apenas teoria elementar dos números, e a outra utilizando os métodos da teoria algébrica dos números.

Comecemos pela demonstração sem o uso dos conceitos de teoria algébrica dos números. Essa construção é retirada de $(2, Seção\ 4.1)$.

Teorema 118. *As soluções inteiras da equação:*

$$x^2 + y^2 = z^2$$

são da forma:

$$x = \pm d(m^2 - n^2), y = \pm 2mnd \text{ e } z = \pm d(m^2 + n^2)$$

Ou

$$x = \pm 2mnd, y = \pm d(m^2 - n^2) \text{ e } z = \pm d(m^2 + n^2)$$

Com $m, n \in \mathbb{N}$, $(m, n) = 1$ *e* $d \in \mathbb{N}$.

Demonstração. Seja $(x, y, z) \in \mathbb{Z}^3$ uma solução. Note que (y, x, z) também é uma solução (por isso encontramos duas formas para as soluções no enunciado). Primeiramente, podemos supor que $(x, y) = (y, z) = (x, z) = 1$. De fato, suponha que $(x, y) = d \neq 1$. Então:

$$z^2 = x^2 + y^2 = d^2x'^2 + d^2y'^2 = d^2(x'^2 + y'^2)$$

Donde $d^2 \mid z^2$. Assim, $d \mid z$. Logo, $z = dz'$ e:

$$d^2z'^2 = d^2(x'^2 + y'^2) \Rightarrow z'^2 = x'^2 + y'^2$$

Portanto, (x', y', z') é solução da equação e $(x', y') = 1$. Repetindo esse processo para (y, z) e (x, z), encontramos uma solução (x, y, z) com $(x, y) = (y, z) = (x, z)$. Note ainda que a solução original (sem a condição que os MDCs sejam iguais a 1) é da forma (dx, dy, dz), com $d \in \mathbb{N}$. Logo, se encontrarmos as soluções dessa equação com x, y, z primos entre si dois-a-dois, teremos encontrado todas as soluções inteiras. Podemos ainda supor que $x, y, z \geq 0$, pois se (x, y, z) é solução, $(\pm x, \pm y, \pm z)$ também é.

Com isso, seja (x, y, z) com $x, y, z \geq 0$ primos entre si dois-a-dois uma solução. Temos que x e y não podem ser ambos pares. Sem perda de generalidade, podemos supor que x é ímpar. Ainda, como $a^2 \equiv 0$ ou $1 \pmod 4$ para todo $a \in \mathbb{Z}$, temos que y não pode ser ímpar, pois, neste caso, teríamos:

$$z^2 \equiv x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4$$

o que seria um absurdo. Assim, y é par. Por outro lado, temos:

$$y^2 = z^2 - x^2 = (z - x)(z + x)$$

Como $(z, z + x) = (z, x) = 1$, temos $(z - x, z + x) = (2z, z + x) = (2, z + x) = 2$ (pois z e x são ímpares). Assim, a equação acima se torna:

$$\frac{y^2}{2^2} = \frac{z - x}{2} \times \frac{z + x}{2}$$

Com $\frac{z - x}{2}, \frac{z + x}{2}, \frac{y}{2} \in \mathbb{Z}$ e $\left(\frac{z - x}{2}, \frac{z + x}{2}\right) = 1$. Como o produto de $\frac{z + x}{2}$ e $\frac{z - x}{2}$ é um quadrado perfeito, temos pelo Teorema Fundamental da Aritmética que $\frac{z + x}{2}$ e $\frac{z - x}{2}$ são quadrados perfeitos. Assim, existem $m, n \in \mathbb{N}$ tais que:

$$\frac{z + x}{2} = m^2, \frac{z - x}{2} = n^2$$

Com isso, temos:

$$\left(\frac{y}{2}\right)^2 = m^2n^2 \Rightarrow \frac{y}{2} = mn \Rightarrow y = 2mn$$

Como $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$, temos $(m, n) = 1$. Somando e subtraindo as equações:

$$\frac{z+x}{2} = m^2 \text{ e } \frac{z-x}{2} = n^2$$

encontramos:

$$x = m^2 - n^2 \text{ e } z = m^2 + n^2$$

Assim, todas as soluções (x, y, z) com $x, y, z \geq 0$ primos entre si dois-a-dois são da forma

$$x = m^2 - n^2, y = 2mn \text{ e } z = m^2 + n^2$$

com $m, n \in \mathbb{N}$, $(m, n) = 1$. Como vimos, qualquer outra solução da equação pode ser obtida multiplicando x, y e z por uma constante $d \in \mathbb{N}$, trocando x com y e invertendo os sinais de x, y e z arbitrariamente. Portanto, temos que toda solução inteira da equação $x^2 + y^2 = z^2$ é da forma:

$$x = \pm d(m^2 - n^2), y = \pm 2mnd \text{ e } z = \pm d(m^2 + n^2)$$

ou da forma:

$$x = \pm 2mnd, y = \pm d(m^2 - n^2) \text{ e } z = \pm d(m^2 + n^2)$$

com $m, n \in \mathbb{N}$, $(m, n) = 1$ e $d \in \mathbb{N}$. Por fim, basta notar que se $m, n, d \in \mathbb{N}$ e $(m, n) = 1$, então:

$$\begin{aligned}(\pm d(m^2 - n^2))^2 + (\pm 2mnd)^2 &= (\pm 2mnd)^2 + (\pm d(m^2 - n^2))^2 = \\ &= d^2(m^4 - 2m^2n^2 + 4m^2n^2 + n^4) = d^2(m^4 + 2m^2n^2 + n^4) = \\ &= (\pm d(m^2 + n^2))^2\end{aligned}$$

donde toda expressão de uma das formas mencionadas é, de fato, uma solução da equação. □

Daremos agora uma demonstração alternativa, utilizando os conceitos e resultados do capítulo 1, para evidenciar a utilidade da teoria estudada na resolução de equações diofantinas.

Teorema 119. *As soluções inteiras da equação:*

$$x^2 + y^2 = z^2$$

são da forma:

$$x = \pm d(m^2 - n^2), y = \pm 2mnd \text{ e } z = \pm d(m^2 + n^2)$$

Ou

$$x = \pm 2mnd, y = \pm d(m^2 - n^2) \text{ e } z = \pm d(m^2 + n^2)$$

Com $m, n \in \mathbb{N}$, $(m, n) = 1$ e $d \in \mathbb{N}$.

Demonstração. Pelas mesmas considerações da demonstração anterior, podemos estudar as soluções $(x, y, z) \in \mathbb{Z}^3$ com $x, y, z \geq 0$ primos entre si dois-a-dois. Sabemos que $\mathbb{Z}+\mathbb{Z}i$ é um domínio Euclidiano, donde, pelo Teorema 18, $\mathbb{Z}+\mathbb{Z}i$ é um domínio de ideais principais e pelo Teorema 38, $\mathbb{Z}+\mathbb{Z}i$ é um domínio de fatoração única. Assim, podemos reescrever a equação original como sendo:

$$z^2 = (x + yi)(x - yi)$$

Note que $(x, x - yi) = (x, -yi) = (x, -i) = (x, i) = 1$ pois $(x, y) = 1$ e $i \in U(\mathbb{Z} + \mathbb{Z}i)$. Pelas mesmas considerações da demonstração anterior, sabemos que x é ímpar e y é par ou x é par e y é ímpar. Supomos então, sem perda de generalidade, que x é ímpar. Portanto:

$$\langle x + yi, x - yi\rangle = \langle 2x, x - yi\rangle = \langle 2, x - yi\rangle = \langle a + bi\rangle$$

com $a, b \in \mathbb{Z}$, pois $\mathbb{Z}+\mathbb{Z}i$ é domínio de ideais principais. Primeiramente, note que $2 \nmid x-yi$, pois $2(r + si) = 2r + 2si$ para todos $r, s \in \mathbb{Z}$ e x não é par. Assim, como $a + bi \mid 2, x - yi$, temos $a + bi \not\sim 2$. Dessa forma, como $a + bi \mid 2$, temos:

$$a^2 + b^2 \mid 4 \text{ e } a + bi \not\sim 2 \Rightarrow a^2 + b^2 = 1 \text{ ou } a^2 + b^2 = 2$$

Suponha que $a^2 + b^2 = 2$. Neste caso, devemos ter $a^2 = b^2 = 1$, donde $a + bi \in \{1+i, 1-i, -1+i, -1-i\}$. Note que $-1-i = -(1+i)$, $1-i = -i(1+i)$ e $-1+i = i(1+i)$, donde todos os elementos acima são associados. Portanto, podemos tomar $a+bi = 1+i$ sem perda de generalidade. Note que, dados $r, s \in \mathbb{Z}$, temos $(1 + i)(r + si) = (r - s) + (r + s)i$ e $r - s \equiv r + s \pmod 2$. Portanto, como $1 + i = a + bi \mid x - yi$, temos $1 \equiv x \equiv -y \equiv 0 \pmod 2$, o que é um absurdo. Logo, devemos ter $a^2 + b^2 = 1$, donde $a + bi$ é uma unidade e, portanto, $(x + yi, x - yi) = 1$ (isto é, $x + yi$ e $x - yi$ são primos entre si). Como $\mathbb{Z}+\mathbb{Z}i$ é um domínio de fatoração única, $x + yi$ e $x - yi$ são primos entre si e seu produto é um quadrado perfeito, temos que $x + yi$ e $x - yi$ são quadrados perfeitos. Portanto, existem $m, n \in \mathbb{Z}$ tais que:

$$x + yi = (m + ni)^2$$
$$x - yi = (m - ni)^2$$

Da primeira equação, segue que:

$$x + yi = m^2 + 2mni - n^2$$

igualando os coeficientes, encontramos:

$$x = m^2 - n^2 \text{ e } y = 2mn$$

Donde segue que $z = m^2 + n^2$. Note que podemos supor $m, n \in \mathbb{N}$. De fato, se $n = 0$, temos $y = 0$ e $x = m^2 = (\pm m)^2 = z$, donde podemos assumir que $m \geq 0$. Se $m = 0$, temos $x = -n^2$. Como estamos assumindo que a solução é tal que $x, y, z \geq 0$, temos $n = 0$. Se

$m, n \neq 0$, como $y = 2mn \geq 0$, temos $m, n > 0$ ou $m, n < 0$. Caso $m, n < 0$, tomemos $m' = -m$ e $n' = -n$. Neste caso, segue que $m', n' \in \mathbb{N}$ e $x = m^2 - n^2 = (m')^2 - (n')^2$ e $y = 2mn = 2m'n'$, donde $z = (m')^2 + (n')^2$. Dessa forma, podemos assumir que $m, n \in \mathbb{N}$. Afirmo ainda que $(m, n) = 1$. De fato, se $(m, n) \neq 1$, seja $p \in \mathbb{Z}$ um primo com $p \mid (m, n)$. Então $p \mid m, n$, donde $p \mid x = m^2 - n^2$ e $p \mid 2mn = y$. Assim, $p \mid (x, y) = 1$, o que é absurdo. Portanto, $(m, n) = 1$. Pelas mesmas considerações feitas ao final da demonstração anterior (com relação à encontrar soluções e à verificar se as formas apresentadas são de fato soluções), o resultado segue. □

7.5 A EQUAÇÃO $x^m = y^2 + k$

Usaremos agora os conceitos do capítulo 2 para estudar casos específicos da equação $x^m = y^2 + k$, com $m \in \mathbb{N}$ e $k \in \mathbb{Z}$. Note que, na (7.2), estudamos mais a fundo o caso em que $m = 3$, utilizando as ferramentas desenvolvidas ao longo de todo o texto. Mostraremos, num teorema proposto pelo autor deste texto, que para certos valores de k, utilizando apenas os conceitos do capítulo 1, conseguimos encontrar resultados que valem para todo $m \geq 2$.

Teorema 120. *Sejam $k \in \mathbb{N}^*$ livre de quadrados com $k > 2$ tal que $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$ é um domínio de fatoração única e $m \in \mathbb{Z}$ par com $m \geq 2$. Então a equação $x^m = y^2 + k$ não possui solução inteira.*

Demonstração. Seja $(x, y) \in \mathbb{Z}^2$ uma solução de:

$$x^m = y^2 + k$$

Primeiramente, note que $(y, k) = 1$. De fato, suponha que $(y, k) \neq 1$. Então existe $p \in \mathbb{Z}$ primo com $p \mid y, k$. Logo:

$$p \mid y^2 + k = x^m \Rightarrow p \mid x$$

Dessa forma, como $m \geq 2$, temos:

$$p^2 \mid x^m - y^2 = k$$

Mas k é livre de quadrados, o que é um absurdo. Assim, $(y, k) = 1$. Reescrevamos a equação acima como sendo:

$$x^m = (y + \sqrt{-k})(y - \sqrt{-k})$$

Note que:

$$(y + \sqrt{-k}, y - \sqrt{-k}) = (y + \sqrt{-k}, 2y) = (y + \sqrt{-k}, 2)$$

pois $(y + \sqrt{-k}, y) = (y, \sqrt{-k})$. Como $(y, k) = 1$ (em $\mathbb{Z}$), existem $r, s \in \mathbb{Z}$ tais que $yr + ks = y(r + 0\sqrt{-k}) + (0 - s\sqrt{-k})\sqrt{-k} = 1$, donde $1 \in \left\langle y, \sqrt{-k} \right\rangle$ e, consequentemente,

$(y, \sqrt{-k}) = 1$. Mostremos então que $(y + \sqrt{-k}, 2) = 1$. De fato, note que, dados $u, v \in \mathbb{Z}$, $2(u + v\sqrt{-k}) = 2u + 2v\sqrt{-k}$. Como o coeficiente de $\sqrt{-k}$ em $y + \sqrt{-k}$ é 1 e $2 \nmid 1$, segue que $2 \nmid y + \sqrt{-k}$. Assim, $(y + \sqrt{-k}, 2) \not\sim 2$ e $(y + \sqrt{-k}, 2) \mid 2$. Mostremos que 2 é irredutível em $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$. De fato, se $u + v\sqrt{-k} \mid 2$, temos pela função ϕ_{-k} que:

$$u^2 + kv^2 \mid 4$$

Se 2 for redutível, então podemos encontrar $u, v \in \mathbb{Z}$ tais que $u^2 + kv^2 \neq 1, 4$. Neste caso, deveremos ter $u^2 + kv^2 = 2$, o que é um absurdo. De fato, se $v \neq 0$, temos $u^2 + kv^2 \geq kv^2 \geq k > 2$, donde devemos ter $v = 0$ e $u^2 = 2$, donde $u = \pm\sqrt{2} \notin \mathbb{Z}$. Assim, 2 é irredutível em $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$. Como $(y + \sqrt{-k}, 2) \mid 2$, $(y + \sqrt{-k}, 2) \not\sim 2$ e $(y + \sqrt{-k}, 2) \in \mathbb{Z} + \mathbb{Z}\sqrt{-k}$, segue da irredutibilidade de 2 que $(y + \sqrt{-k}, 2) = 1$, donde $y + \sqrt{-k}$ e $y - \sqrt{-k}$ são coprimos. Com isso, e os fatos de que $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$ é domínio de fatoração única e de que o produto de $y + \sqrt{-k}$ e de $y - \sqrt{-k}$ é uma m-ésima potência, segue que $y + \sqrt{-k}$ e $y + \sqrt{-k}$ são m-ésimas potências em $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$. Em particular, existem $a, b \in \mathbb{Z}$ tais que:

$$y + \sqrt{-k} = (a + b\sqrt{-k})^m$$

Como m é par e $m \geq 2$, existe $n \in \mathbb{N}^*$ tal que $m = 2n$. Assim, a equação acima pode ser reescrita como:

$$y + \sqrt{-k} = (a + b\sqrt{-k})^{2n} = ((a^2 - kb^2) + 2ab\sqrt{-k})^n$$

Expandindo a expressão da direita como um binômio de Newton, temos:

$$y + \sqrt{-k} = \sum_{i=0}^{n} \binom{n}{i} (a^2 - kb^2)^i (2ab\sqrt{-k})^{n-i}$$

Analisaremos o coeficiente de $\sqrt{-k}$ na expressão acima. Sabemos que um termo no somatório a direita contribui para o coeficiente de $\sqrt{-k}$ se o expoente $n - i$ é ímpar. Seja então $i \in \{0, ..., n\}$ tal que $n - i$ seja ímpar. Então, $n - i \geq 1$, donde $n - i - 1 \in \mathbb{N}$. Assim, temos:

$$\binom{n}{i} (a^2 - kb^2)^i (2ab\sqrt{-k})^{n-i} = \binom{n}{i} (a^2 - kb^2)^i (2ab)^{n-i} (\sqrt{-k})^{n-i} =$$
$$= \binom{n}{i} (a^2 - kb^2)^i 2ab\sqrt{-k} (2ab\sqrt{-k})^{n-i-1} = 2ab \left(\binom{n}{i} (a^2 - kb^2)^i (2ab\sqrt{-k})^{n-i-1} \right) \sqrt{-k}$$

Portanto, 2 divide o coeficiente deste termo. Assim, a soma dos termos desta forma (a qual é igual ao coeficiente de $\sqrt{-k}$ em $y + \sqrt{-k}$) é divisível por 2. Entretanto, o coeficiente de $\sqrt{-k}$ em $y + \sqrt{-k}$ é 1, donde segue que $2 \mid 1$, o que é um absurdo. Dessa forma, a equação $x^m = y^2 + k$ não possui solução. □

Note que o Teorema 120 também nos dá um critério para determinar se um domínio da forma $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$ é um domínio de fatoração única, quando $k > 2$ é livre de quadrados.

Em particular, se a equação $x^2 = y^2 + k$ tem solução, então $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$ não é domínio de fatoração única. Neste sentido, por exemplo, $\mathbb{Z} + \mathbb{Z}\sqrt{-k}$ não é domínio de fatoração única quando k é ímpar livre de quadrados. De fato, existem $a, b \in \mathbb{Z}$ ímpares tais que $k = ab$. Como k é livre de quadrados, $a \neq b$, digamos $a < b$. Assim, tomando $x = (a + b)/2$ e $y = (b - a)/2$, temos $(x - y)(x + y) = ba = k$.

7.6 A EQUAÇÃO $x^2 - my^2 = N$

Por fim, estudaremos a equação $x^2 - my^2 = N$. Neste estudo, utilizaremos apenas de métodos da teoria elementar dos números. Esta escolha foi feita pelo fato de que, apesar dessa equação poder ser resolvida por ambos os métodos (isto é, com teoria elementar dos números e com teoria algébrica dos números), tal resolução faz uso, em ambos os casos, de frações contínuas, as quais fogem do escopo deste texto. Por isso, apresentaremos apenas propriedades básicas desse tipo de equação, com o intuito de apresentar uma condição necessária e outra suficiente para a existência de soluções desse tipo de equação. E para tais resultados, necessitamos apenas da teoria elementar dos números.

Comecemos com uma proposição que nos permite construir soluções da equação acima a partir de outras soluções.

Proposição 22. *Sejam $a, b, m \in \mathbb{Z}$ tais que existem $x, y, u, v \in \mathbb{Z}$ com $x^2 - my^2 = a$ e $u^2 - mv^2 = b$. Então existem $p, q \in \mathbb{Z}$ tais que $p^2 - mq^2 = ab$. Analogamente, se $a = my^2 - x^2$ e $b = u^2 - mv^2$, então existem $p, q \in \mathbb{Z}$ tais que $mq^2 - p^2 = ab$.*

Demonstração. Para o primeiro caso, temos:

$$\begin{aligned} ab &= \left(x^2 - my^2\right)\left(u^2 - mv^2\right) = x^2u^2 - mx^2v^2 - mu^2y^2 + m^2y^2v^2 \\ &= x^2u^2 + 2mxyuv + m^2y^2v^2 - mu^2y^2 - 2mxyuv - mx^2v^2 \\ &= (xu + myv)^2 - m\left(u^2y^2 + 2xyuv + x^2v^2\right) \\ &= (xu + myv)^2 - m\,(uy + xv)^2 = (xu - myv)^2 - m\,(uy - xv)^2 \end{aligned}$$

Assim, fazendo $p = xu + myv$ e $q = uy + xv$, ambos inteiros (ou $p = xu - myv$ e $q = uy - xv$), temos:

$$p^2 - mq^2 = ab$$

Para o segundo caso, temos:

$$\begin{aligned} ab &= \left(-x^2 + my^2\right)\left(u^2 - mv^2\right) = -x^2u^2 + mx^2v^2 + mu^2y^2 - m^2y^2v^2 \\ &= -\left(x^2u^2 + 2mxyuv + m^2y^2v^2 - mu^2y^2 - 2mxyuv - mx^2v^2\right) \\ &= -\left((xu + myv)^2 - m\left(u^2y^2 + 2xyuv + x^2v^2\right)\right) \\ &= -(xu + myv)^2 + m\,(uy + xv)^2 = -(xu - myv)^2 + m\,(uy - xv)^2 \end{aligned}$$

Assim, fazendo $p = xu + myv$ e $q = uy + xv$, ambos inteiros (ou $p = xu - myv$ e $q = uy - xv$), temos:

$$mq^2 - p^2 = ab$$

□

Dado $a \in \mathbb{Z}$, diremos que a é uma m-solução caso existam $x, y \in \mathbb{Z}$ tais que $x^2 - my^2 = a$ ou $my^2 - x^2 = a$.

Note que o caso $m = 0$ possui solução se, e somente se, N for um quadrado perfeito (em particular, devemos ter $N \geq 0$). Note ainda que, se $N = 0$, a equação sempre possui a solução $x = y = 0$, a qual chamaremos de solução trivial. Entretanto, existem certos valores de m para os quais há soluções não-triviais. Estes casos serão analisados na seguinte proposição.

Proposição 23. *A equação $x^2 - my^2 = 0$ possui solução não-trivial se, e somente se, m é um quadrado perfeito.*

Demonstração. ($\Rightarrow$) Seja $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ uma solução não trivial de $x^2 = my^2$. Se $x = 0$, devemos ter $my^2 = 0$. Sendo (x, y) solução não trivial, não podemos ter $y = 0$, donde segue que a equação admite solução não trivial apenas se $m = 0$, e 0 é quadrado perfeito. Se $x \in \{-1, 1\}$, temos $my^2 = 1$, donde $m \mid 1 \Rightarrow m = \pm 1$. Mas $y^2 \geq 0$ para todo $y \in \mathbb{Z}$ e $1 = my^2 > 0$. Assim, não podemos ter $m < 0$, donde segue que $m = 1 = 1^2$. Se $x \notin \{0, -1, 1\}$, sabemos pelo Algoritmo de Euclides que x possui uma fatoração em primos. Seja $x = u \prod_{i=1}^{n} p_i^{\alpha_i}$ esta fatoração, com $n \in \mathbb{N}$, $u \in \{-1, 1\}$, $p_1, ..., p_n \in \mathbb{N}$ primos e $\alpha_1, ..., \alpha_n \in \mathbb{N}$. Assim, $my^2 = x^2 = u^2 \prod_{i=1}^{n} p_i^{2\alpha_i} = \prod_{i=1}^{n} p_i^{2\alpha_i} \neq 0$, donde $m, y \neq 0$. Dessa forma, dado $i \in \{1, ..., n\}$, temos:

$$\nu_{p_i}\left(x^2\right) = 2\nu_{p_i}(x) = \nu_{p_i}\left(my^2\right) = \nu_{p_i}(m) + 2\nu_{p_i}(y) \Rightarrow$$
$$\nu_{p_i}(m) = 2\left(\nu_{p_i}(x) - \nu_{p_i}(y)\right)$$

em que $\nu_{p_i}(h)$ é o maior expoente de p_i que divide h. Portanto, $\nu_{p_i}(m) \equiv 0 \pmod 2$ para todo $i \in \{1, ..., n\}$, donde m é quadrado perfeito.

($\Leftarrow$) Se m é quadrado perfeito, existe $k \in \mathbb{Z}$ tal que $m = k^2$. Dado $y \in \mathbb{Z} \setminus \{0\}$, tomemos $x = ky \in \mathbb{Z}$. Então $(x, y) \neq (0, 0)$ (pois $y \neq 0$) e $x^2 - my^2 = (ky)^2 - k^2y^2 = 0$, donde (x, y) é solução não-trivial. □

Daremos agora uma condição suficiente e outra necessária para que uma equação da forma $x^2 - my^2 = N$ tenha solução com $x, y \in \mathbb{Z}$ para $m, N \neq 0$. Ambas foram propostas pelo autor deste texto. Começaremos pela condição suficiente.

Teorema 121. *Sejam $m, N \in \mathbb{Z} \setminus \{0\}$, $N = ud^2l$ a decomposição em parte livre de quadrados e $l = \prod_{i=1}^{n} p_i$ a fatoração em primos de l. Se $u, p_1, ..., p_n$ são m-soluções e $\#\{x \in \{u, p_1, ..., p_n\} \mid x = ma^2 - b^2, \text{ com } a, b \in \mathbb{Z}\} \equiv 0 \pmod 2$, a equação $x^2 - my^2 = N$ possui solução.*

Demonstração. Como $\#\{x \in \{u, p_1, ..., p_n\} \mid x = ma^2 - b^2, \text{ com } a, b \in \mathbb{Z}\} \equiv 0 \pmod 2$, existe $k \in \mathbb{N} \cup \{0\}$ tal que $\#\{x \in \{u, p_1, ..., p_n\} \mid x = ma^2 - b^2, \text{ com } a, b \in \mathbb{Z}\} = 2k$. Podemos então enumerar os termos deste conjunto como sendo $\{x \in \{u, p_1, ..., p_n\} \mid x = ma^2 - b^2, \text{ com } a, b \in \mathbb{Z}\} = \{x_1, x_2, ..., x_{2k}\}$. Iremos parear cada um destes termos nos pares (x_i, x_{2k+1-i}), com $i \in \{1, ..., k\}$. Para todo $i \in \{1, ..., 2k\}$, existem $a_i, b_i \in \mathbb{Z}$ tais que $x_i = mb_i^2 - a_i^2$. Assim, dado $i \in \{1, ..., k\}$, temos:

$$\begin{aligned} x_i x_{2k+1-i} &= \left(mb_i^2 - a_i^2\right)\left(mb_{2k+1-i}^2 - a_{2k+1-i}^2\right) = (-1)\left(a_i^2 - mb_i^2\right)(-1)\left(a_{2k+1-i}^2 - mb_{2k+1-i}^2\right) \\ &= \left(a_i^2 - mb_i^2\right)\left(a_{2k+1-i}^2 - mb_{2k+1-i}^2\right) \end{aligned}$$

Pela Proposição 22, existem $A_i, B_i \in \mathbb{Z}$ tais que $x_i x_{2k+1-i} = A_i^2 - mB_i^2$. Seja $\{y_1, ..., y_h\} = \{u, p_1, ..., p_n\} \setminus \{x \in \{u, p_1, ..., p_n\} \mid x = ma^2 - b^2, \text{ com } a, b \in \mathbb{Z}\}$. Para cada $i \in \{1, ..., h\}$, existem $U_i, V_i \in \mathbb{Z}$ tais que $y_i = U_i^2 - mV_i^2$. Dessa forma:

$$\begin{aligned} ul = u\prod_{i=1}^{n} p_i &= \left(\prod_{i=1}^{2k} x_i\right)\left(\prod_{i=1}^{h} y_i\right) = \left(\prod_{i=1}^{k} x_i x_{2k+1-i}\right)\left(\prod_{i=1}^{h} y_i\right) \\ &= \left(\prod_{i=1}^{k}\left(A_i^2 - mB_i^2\right)\right)\left(\prod_{i=1}^{h}\left(U_i^2 - mV_i^2\right)\right) \end{aligned}$$

Aplicando a Proposição 22 repetidamente, existem $X, Y \in \mathbb{Z}$ tais que $ul = X^2 - mY^2$. Fazendo $x = Xd$ e $y = Yd$, temos $x, y \in \mathbb{Z}$ e $N = ud^2l = d^2\left(X^2 - mY^2\right) = (dX)^2 - m\left(dY\right)^2 = x^2 - my^2$. □

Daremos agora uma condição necessária para que haja uma solução da equação $x^2 - my^2 = N$.

Teorema 122. *Sejam $m, N \in \mathbb{Z} \setminus \{0\}$, $N = ud^2l$ a decomposição em parte livre de quadrados, $l = \prod_{i=1}^{n} p_i$ a fatoração em primos de l e $p \in \mathbb{N}$ um primo. Se a equação $x^2 - my^2 = N$ tem solução, segue que:*

1. *Se $p \mid m$ e $p \nmid N$, então $\#\left\{x \in \{u, p_1, ..., p_n\} \mid \left(\frac{x}{p}\right) = -1\right\} \equiv 0 \pmod 2$.*
2. *Se $p \mid N$ e $p \nmid m$, então $\left(\frac{m}{p}\right) = 1$ ou $p^2 \mid N$ e a equação $x^2 - my^2 = \frac{N}{p^2}$ tem solução.*
3. *Se $p \mid m$ e $p \| N$, então $p \| m$ e a equação $px^2 - \frac{m}{p}y^2 = \frac{N}{p}$ possui solução.*

4. *Se* $p \| m$ *e* $p \mid N$*, então* $p \| N$ *ou* $p^2 \mid N$ *e a equação* $x^2 - my^2 = \dfrac{N}{p^2}$ *tem solução.*

5. *Se* $p^2 \mid m, N$*, então a equação* $x^2 - \dfrac{m}{p^2}y^2 = \dfrac{N}{p^2}$ *tem solução.*

Demonstração. Seja $(x, y) \in \mathbb{Z}^2$ uma solução da equação:

$$x^2 - my^2 = N \tag{7.31}$$

a qual existe por hipótese.

1. Analisemos a equação (7.31) módulo p:

   $$x^2 \equiv x^2 - my^2 \equiv N \pmod{p}$$

   pois $p \mid m$. Como $p \nmid N$, segue que $p \nmid x$, donde:

   $$\left(\frac{N}{p}\right) = \left(\frac{x^2}{p}\right) = 1$$

   Sejam

   $$\{x_1, ..., x_k\} = \left\{x \in \{u, p_1, ..., p_n\} \mid \left(\frac{x}{p}\right) = -1\right\}$$

   $$\{y_1, ..., y_l\} = \{u, p_1, ..., p_n\} \setminus \left\{x \in \{u, p_1, ..., p_n\} \mid \left(\frac{x}{p}\right) = -1\right\}$$

   Pelas propriedades do símbolo de Legendre (as quais podem ser encontradas em (2)), temos:

   $$\left(\prod_{i=1}^{l}\left(\frac{y_i}{p}\right)\right)\left(\prod_{i=1}^{k}\left(\frac{x_i}{p}\right)\right) = \left(\frac{N}{p}\right) = 1$$

   Em particular, $\left(\dfrac{y_i}{p}\right) \neq 0$ para todo $i \in \{1, ..., l\}$. Como $\left(\dfrac{y_i}{p}\right) = -1$ implicaria em $y_i \in \left\{x \in \{u, p_1, ..., p_n\} \mid \left(\dfrac{x}{p}\right) = -1\right\}$ (o que seria um absurdo), temos $\left(\dfrac{y_i}{p}\right) = 1$ para todo $i \in \{1, ..., l\}$. Ainda, pela definição de $\left\{x \in \{u, p_1, ..., p_n\} \mid \left(\dfrac{x}{p}\right) = -1\right\}$, temos $\left(\dfrac{x_i}{p}\right) = -1$ para todo $i \in \{2, ..., k\}$. Assim:

   $$\left(\prod_{i=1}^{l}\left(\frac{y_i}{p}\right)\right)\left(\prod_{i=1}^{k}\left(\frac{x_i}{p}\right)\right) = 1^l(-1)^k = (-1)^k = 1$$

   donde segue que $k \equiv 0 \pmod 2$. Entretanto, $k = \#\left\{x \in \{u, p_1, ..., p_n\} \mid \left(\dfrac{x}{p}\right) = -1\right\}$, logo temos o resultado.

2. Suponha que $\left(\frac{m}{p}\right) \neq 1$. Então, como $p \nmid m$, temos $\left(\frac{m}{p}\right) = -1$. Assim, analisando a equação (7.31) módulo p, temos:

$$x^2 - my^2 \equiv N \equiv 0 \pmod{p} \Rightarrow x^2 \equiv my^2 \pmod{p}$$

Com isso:

$$\left(\frac{x^2}{p}\right) = \left(\frac{my^2}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{y^2}{p}\right) = -\left(\frac{y^2}{p}\right)$$

Como $\left(\frac{z^2}{p}\right) \geq 0$ para todo $z \in \mathbb{Z}$, temos $\left(\frac{x^2}{p}\right) \geq 0 \geq -\left(\frac{y^2}{p}\right)$. Como vale a igualdade entre esses termos, devemos ter $\left(\frac{x^2}{p}\right) = 0 = -\left(\frac{y^2}{p}\right)$, donde segue que $p \mid x, y$. Neste caso, $p^2 \mid x^2 - my^2 = N$. Sejam $x' = \frac{x}{p} \in \mathbb{Z}$ e $y' = \frac{y}{p} \in \mathbb{Z}$. Então:

$$(x')^2 - m(y')^2 = \left(\frac{x}{p}\right)^2 - m\left(\frac{y}{p}\right)^2 = \frac{x^2 - my^2}{p^2} = \frac{N}{p^2}$$

donde $(x', y') \in \mathbb{Z}^2$ é solução de:

$$x^2 - my^2 = \frac{N}{p^2}$$

3. Como $p \mid m, N$, temos $p \mid x^2 = N + my^2$, donde $p \mid x$ e $p^2 \mid x^2$. Suponha que $p \| m$ seja falso. Então, como $p \mid m$, temos que $p^2 \mid m$. Dessa forma, $p^2 \mid x^2 - my^2 = N$, o que é um absurdo. Assim, $p \| m$. Seja $x' = \frac{x}{p} \in \mathbb{Z}$. Então:

$$px'^2 - \frac{m}{p}y^2 = p\left(\frac{x^2}{p^2}\right) - \frac{m}{p}y^2 = \left(\frac{x^2 - my^2}{p}\right) = \frac{N}{p}$$

donde $(x', y) \in \mathbb{Z}^2$ é uma solução de:

$$px^2 - \frac{m}{p}y^2 = \frac{N}{p}$$

4. Suponha que $p \| N$ seja falso. Então, como $p \mid N$, temos $p^2 \mid N$. Ainda, como $p \mid m$, segue que $p \mid x^2 = my^2 + N$. Uma vez que p é primo, temos $p \mid x$. Portanto:

$$p^2 \mid my^2 = x^2 - N$$

Como $p \| m$, temos que $p^2 \nmid m$. Assim, $p \mid y^2$, donde $p \mid y$. Sejam $x' = \frac{x}{p} \in \mathbb{Z}$ e $y' = \frac{y}{p} \in \mathbb{Z}$. Então:

$$(x')^2 - m(y')^2 = \left(\frac{x}{p}\right)^2 - m\left(\frac{y}{p}\right)^2 = \frac{x^2 - my^2}{p^2} = \frac{N}{p^2}$$

donde $(x', y') \in \mathbb{Z}^2$ é solução da equação:

$$x^2 - my^2 = \frac{N}{p^2}$$

5. Se $p^2 \mid m, N$, então $p^2 \mid x^2 = N + my^2$, donde $p \mid x$. Seja $x' = \dfrac{x}{p} \in \mathbb{Z}$. Segue que:

$$(x')^2 - \frac{m}{p^2}y^2 = \left(\frac{x}{p}\right)^2 - \frac{m}{p^2}y^2 = \frac{x^2 - my^2}{p^2} = \frac{N}{p^2}$$

donde $(x', y) \in \mathbb{Z}^2$ é solução da equação:

$$x^2 - \frac{m}{p^2}y^2 = \frac{N}{p^2}$$

□

Note que, no resultado anterior, muitas vezes conseguimos reduzir a equação para outra mais simples, sendo que, exceto no caso do item 3, essa nova equação ainda é da forma $x^2 - my^2 = N$, o que nos permite aplicar, novamente, o teorema anterior.

8 CONCLUSÃO

Pudemos notar ao longo deste trabalho que, mesmo para o estudo de equações diofantinas com expoentes pequenos, como as equações $x^3 = y^2 + k$ e $y(y+1) = x(x+1)(x+2)$, é necessário a análise de diversos casos e o uso de uma extensa lista de conceitos e resultados. Tal fato mostra a dificuldade por trás das equações diofantinas, mas também sua elegância, pois estes são problemas facilmente enunciáveis e testáveis computacionalmente, mas que exigem o desenvolvimento e uso de uma extensa teoria algébrica para que possam ser definitivamente resolvidos e categorizados.

Além disso, vimos que, mesmo utilizando apenas a teoria desenvolvida no primeiro capítulo, conseguimos analisar equações importantes e obter resultados sobre essas equações que não seriam facilmente obtidos usando apenas a teoria elementar dos números. Isso nos revela a eficiência da teoria algébrica dos números na resolução de problemas de equações diofantinas.

REFERÊNCIAS

1 Alaca, Ş. and Williams, K. S. *Introductory Algebraic Number Theory*. Cambridge, 2004.

2 Martinez, F. B.; Moreira, C. G.; Saldanha, N. e Tengan, E. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro, IMPA, 5ª edição, 2018.

3 Garcia, A. e Lequain, Y. *Elementos de álgebra*. Rio de Janeiro, IMPA, 2001.